STEPHEN S. KORNICZKY (SB# 135532)
S. CHRISTIAN PLATT (SB# 199318)
SAM TALPALATSKY (SB# 171292)
TREVOR Q. CODDINGTON (SB# 243042)
PAUL, HASTINGS, JANOFSKY & WALKER LLP
3579 Valley Centre Drive
San Diego, CA 92130
Telephone: (858) 720-2500
Facsimile: (858) 720-2555

Attorneys for Plaintiff
DEI HEADQUARTERS, INC.

FILED
DEC 21 2007
CLERK, U.S. DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
BY [signature] DEPUTY

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

DEI HEADQUARTERS, INC., Plaintiff,	CASE NO. '07 CV 2406 BTM RBB
vs.	**COMPLAINT FOR PATENT INFRINGEMENT**
AUTO PAGE, INC. and ADVANCED SECURITY, INC., Defendants.	**DEMAND FOR JURY TRIAL**

ORIGINAL

Plaintiff, by and through its designated attorneys, complains and alleges as follows:

THE PARTIES

1. Plaintiff DEI HEADQUARTERS, INC. ("DEI") is a corporation organized and existing under the laws of the State of Florida and has its principal place of business at One Viper Way, Vista, California 92081.

2. On information and belief, Defendant AUTO PAGE, INC. ("Auto Page") is a corporation organized and existing under the laws of California and has its principal place of business at 960 Knox Street, Unit B, Torrance, California 90502.

3. On information and belief, Defendant ADVANCED SECURITY, INC. ("Advanced Security") is a corporation organized and existing under the laws of Taiwan

and has its principal place of business at 3F, 48 Ta-An Street, His-Chih Taipei Hsien, Taiwan R.O.C.

JURISDICTION AND VENUE

4. This lawsuit is an action for patent infringement. The Court has jurisdiction over the subject matter of this action under 28 U.S.C. §§ 1331 and 1338.

5. This Court has *in personam* jurisdiction as to Autopage because upon information and belief, Auto Page is subject to general and specific jurisdiction in this State. More particularly, upon information and belief, Auto Page engages in systematic and continuous activity in California. Auto Page sells and offers to sell products, including security systems that infringe one or more claims of DEI's patents, in California or places such products in the stream of commerce with the knowledge that the infringing products will be sold in California and this judicial district.

6. This Court has *in personam* jurisdiction as to Advanced Security because upon information and belief, Advanced Security is subject to general and specific jurisdiction in this State. More particularly, upon information and belief, Advanced Security engages in systematic and continuous activity in California. Advanced Security manufactures, sells and offers to sell products, including security systems that infringe one or more claims of DEI's patents, in California or places such products in the stream of commerce with the knowledge that the infringing products will be sold in California and this judicial district.

7. Venue is proper in this judicial district under 28 U.S.C. §§ 1391(b), 1391(c), and 1400(b). Venue is proper in this district under § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim – the alleged infringing activity – occurred and will continue to occur in this judicial district. Venue is proper in this judicial district under § 1391(b)(1) because Auto Page and Advanced Security "reside" in the State of California, and in this judicial district, as the term "reside" is defined in § 1391(c) because Auto Page's and Advanced Security's contacts with this judicial district

are sufficient to render each entity amenable to personal jurisdiction in this district. Venue is proper in this judicial district under § 1400(b) because Auto Page and Advanced Security reside in this district and acts of infringement have occurred within this district.

SUMMARY OF FACTS

DEI and the Patents-In-Suit

8. DEI is a wholly owned subsidiary of Directed Electronics, Inc. ("Directed"). Directed is headquartered in Vista, California and is the world's largest designer, manufacturer, and distributor of automotive security products. Directed has made substantial investments in developing its automotive security technology and has been recognized with many awards for its product innovations.

9. On September 8, 1992, United States Patent No. 5,146,215, entitled "Electronically Programmable Remote Control for Vehicle Security System" issued to assignee Clifford Electronics, Inc. (hereinafter "the '215 patent"). The named inventor on the '215 patent is Ze'ev Drori. A copy of the '215 patent is attached hereto as Exhibit A.

10. On July 22, 1997, United States Patent No. 5,650,774, entitled "Electronically Programmable Remote Control Access System" issued to assignee Clifford Electronics, Inc. (hereinafter "the '774 patent"). The named inventor on the '774 patent is Ze'ev Drori. A copy of the '774 patent is attached hereto as Exhibit B.

11. The '215 patent and the '774 patent were assigned to DEI on January 1, 2003. DEI is the sole and exclusive owner of the '215 patent and the '774 patent.

12. DEI has not granted Autopage or Advanced any license to practice the '215 patent and/or the '774 patent.

Defendant Auto Page

13. Auto Page is a retailer of after-market automotive products including remote control vehicle security systems.

///

14. Auto Page is registered with the Secretary of State's office to do business in California.

15. On information and belief, Auto Page distributes its after-market automotive products through numerous dealers located throughout the United States. In the city of San Diego, Auto Page's automotive products are distributed through at least six dealers identified by Auto Page on its website.

Defendant Advanced Security

16. Advanced Security is a manufacturer of home, car, and motorcycle security system products.

17. On information and belief, Advanced Security distributes, imports, offers for sale and/or sells its security system products to customers and/or retailers throughout California including Auto Page.

FIRST CLAIM

(Infringement of U.S. Patent No. 5,146,215)

18. Plaintiff hereby incorporates by reference paragraphs 1 through 17 as though set forth herein in their entirety.

19. Upon information and belief, Defendants has been and is still directly infringing one or more claims of the '215 patent in violation of 35 U.S.C. § 271 by, without authority, making, using, offering to sell, selling, or importing into the United States remote control vehicle security products and/or systems that embody the invention claimed in the '215 patent.

20. Upon information and belief, Defendants has been and is still directly infringing one or more claims of the '215 patent in violation of 35 U.S.C. § 271 by knowingly and intentionally inducing others to infringe the '215 patent and/or by contributing to the infringement of the '215 patent by others.

///

21. Upon information and belief, Defendants' acts of infringement will continue after service of this complaint.

22. Upon information and belief, Defendants' past and continued infringement of the '215 patent is willful and deliberate, rendering this case appropriate for treble damages under 35 U.S.C. § 284 and making this an exceptional case under 35 U.S.C. § 285.

23. As a result of Defendants' infringement of the '215 patent, Plaintiff has suffered and will suffer damages in the form of lost profits, or at a minimum, will be entitled to recover a reasonable royalty.

24. Unless Defendants are enjoined by this Court from continuing their infringement of the '215 patent, Plaintiff will suffer additional irreparable damages and impairment of the value of its patent rights. Thus, Plaintiff is entitled to an injunction against further infringement.

SECOND CLAIM

(Infringement of U.S. Patent No. 5,650,774)

25. Plaintiff hereby incorporates by reference paragraphs 1 through 17 as though set forth herein in their entirety.

26. Upon information and belief, Defendants have made and/or offered for sale and sold and/or distributed products that infringe directly, by inducement and/or contributory, one or more claims of the '774 patent in violation of 35 U.S.C. § 271.

27. Upon information and belief, Defendants has been and is still directly infringing one or more claims of the '774 patent in violation of 35 U.S.C. § 271 by, without authority, making, using, offering to sell, selling, or importing into the United States remote control vehicle security products and/or systems that embody the invention claimed in the '774 patent.

28. Upon information and belief, Defendants has been and is still directly infringing one or more claims of the '774 patent in violation of 35 U.S.C. § 271 by

knowingly and intentionally inducing others to infringe the '774 patent and/or by contributing to the infringement of the '774 patent by others.

29. Upon information and belief, Defendant's acts of infringement will continue after service of this complaint.

30. Upon information and belief, Defendants' past and continued infringement of the '774 patent is willful and deliberate, rendering this case appropriate for treble damages under 35 U.S.C. § 284 and making this an exceptional case under 35 U.S.C. § 285.

31. As a result of Defendants' infringement of the '774 patent, Plaintiff has suffered and will suffer damages in the form of lost profits, or at a minimum, will be entitled to recover a reasonable royalty.

32. Unless Defendants are enjoined by this Court from continuing their infringement of the '774 patent, Plaintiff will suffer additional irreparable damages and impairment of the value of its patent rights. Thus, Plaintiff is entitled to an injunction against further infringement.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays that judgment be entered by this Court in its favor and against the Defendant, providing the following relief:

A. That judgment be entered that Defendants are infringing the '215 patent and the '774 patent;

B. That Defendants and their agents, servants, employees, successors and assignors, and all those acting under the authority of, or in privity or concert with them, and each of them, be preliminary and permanently enjoined from directly or indirectly infringing the '215 patent and the '774 patent;

C. That judgment be entered for damages, together with prejudgment interest, to compensate Plaintiff for Defendants' infringement of the '215 patent and the '774 patent;

D. That judgment be entered for treble damages pursuant to 35 U.S.C. § 284;

E. That judgment be entered that this case is an exceptional case within the meaning of 35 U.S.C. § 284, and for an award of reasonable attorneys' fees to Plaintiff;

F. That judgment be entered for costs to be awarded to Plaintiff; and

G. For such other and further relief as the Court may deem appropriate under the circumstances.

DATED: December 21, 2007

STEPHEN S. KORNICZKY
S. CHRISTIAN PLATT
SAM TALPALATSKY
TREVOR Q. CODDINGTON
PAUL, HASTINGS, JANOFSKY & WALKER LLP

By: [signature]
TREVOR Q. CODDINGTON

Attorneys for Plaintiff
DEI HEADQUARTERS, INC.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiff Directed Electronics, Inc. respectfully demands a trial by jury as to all issues so triable.

DATED: December 21, 2007

STEPHEN S. KORNICZKY
S. CHRISTIAN PLATT
SAM TALPALATSKY
TREVOR Q. CODDINGTON
PAUL, HASTINGS, JANOFSKY & WALKER LLP

By: [signature]
TREVOR Q. CODDINGTON

Attorneys for Plaintiff
DEI HEADQUARTERS, INC.

EXHIBIT A

US005146215A

United States Patent [19]
Drori

[11] **Patent Number: 5,146,215**
[45] **Date of Patent: Sep. 8, 1992**

[54] **ELECTRONICALLY PROGRAMMABLE REMOTE CONTROL FOR VEHICLE SECURITY SYSTEM**

[75] Inventor: **Ze'ev Drori**, Chatsworth, Calif.

[73] Assignee: **Clifford Electronics, Inc.**, Chatsworth, Calif.

[21] Appl. No.: **277,959**

[22] Filed: **Nov. 30, 1988**

Related U.S. Application Data

[63] Continuation-in-part of Ser. No. 94,395, Sep. 8, 1987, abandoned, and a continuation-in-part of Ser. No. 231,159, Aug. 11, 1988, Pat. No. 4,922,224.

[51] **Int. Cl.**[5] **G06F 7/04**
[52] **U.S. Cl.** **340/825.32**; 340/825.31; 340/825.69; 340/825.72
[58] **Field of Search** 340/825.31, 825.32, 340/825.69, 825.72, 528, 541, 543, 542; 70/278; 361/172; 307/10.2

[56] **References Cited**

U.S. PATENT DOCUMENTS

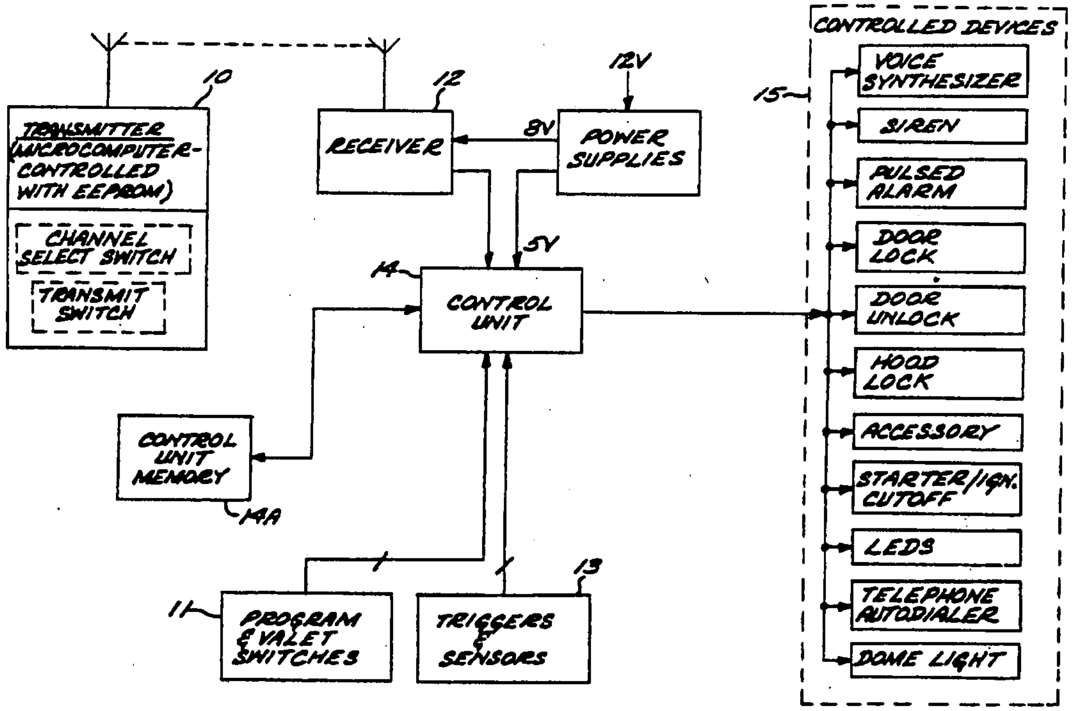
3,337,992 8/1967 Tolson 340/539
4,177,657 12/1979 Aydin 70/278
4,383,242 5/1983 Sassover et al. 340/64
4,535,333 8/1985 Twardowski 340/825.72
4,626,848 12/1986 Ehlers 340/825.72
4,652,860 3/1987 Weishaupt et al. 340/825.31
4,665,397 5/1987 Pinnow 340/825.72
4,754,255 6/1988 Sanders et al. 340/64
4,794,368 12/1988 Grossheim et al. 340/63

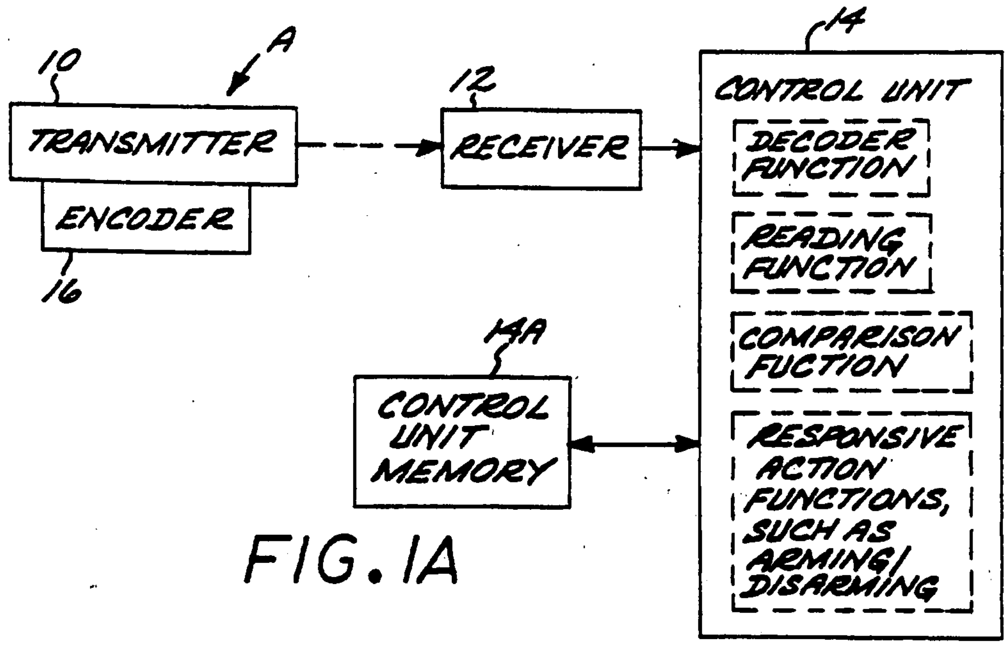
Primary Examiner—Ulysses Weldon
Attorney, Agent, or Firm—Roberts and Quiogue

[57] **ABSTRACT**

An electronically programmable remote control for an vehicle security system. The system remote control comprises one or more hand-held remote transmitters and a receiver unit located in the vehicle. The receiver is operable in conjunction with a control unit which contains a microprocessor capable of performing control functions and encoding functions. The remote control enables the user to electronically program into or delete from the receiver a digital code from any of a plurality of transmitters. It is not necessary for the user or anyone else to know the specific encoded signal which is transmitted from any of the transmitters to the receiver. The receiver is operable with a plurality of transmitters, all of which operate on the same frequency.

10 Claims, 21 Drawing Sheets

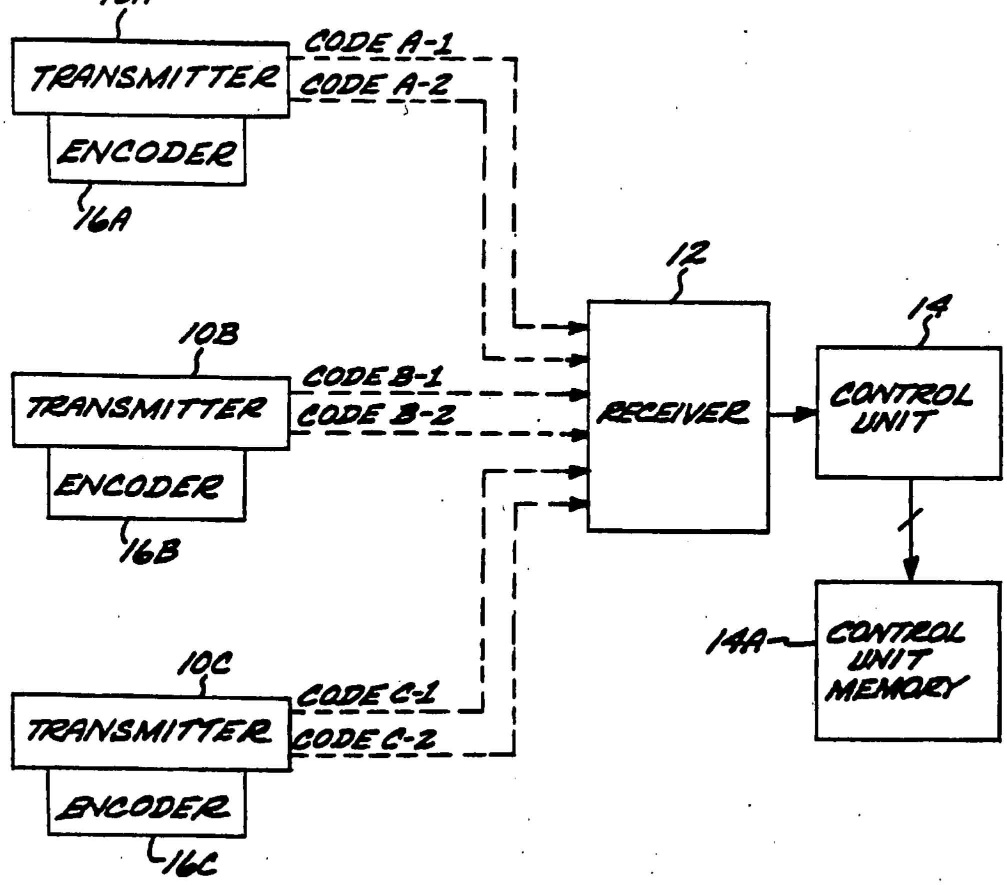

CONTROLLED DEVICES
TRANSMITTER (MICROCOMPUTER-CONTROLLED WITH EEPROM)
CHANNEL SELECT SWITCH
TRANSMIT SWITCH
10
12
RECEIVER
12V
8V
POWER SUPPLIES
5V
14
CONTROL UNIT
15
VOICE SYNTHESIZER
SIREN
PULSED ALARM
DOOR LOCK
DOOR UNLOCK
HOOD LOCK
ACCESSORY
STARTER/IGN. CUTOFF
LEDS
TELEPHONE AUTODIALER
DOME LIGHT
CONTROL UNIT MEMORY
14A
11
PROGRAM & VALET SWITCHES
13
TRIGGERS & SENSORS



A
10
TRANSMITTER
ENCODER
16
12
RECEIVER
14
CONTROL UNIT
DECODER FUNCTION
READING FUNCTION
COMPARISON FUCTION
RESPONSIVE ACTION FUNCTIONS, SUCH AS ARMING/ DISARMING
14A
CONTROL UNIT MEMORY

FIG. 1A

FIG. 2



10A
TRANSMITTER
ENCODER
16A
CODE A-1
CODE A-2
10B
TRANSMITTER
ENCODER
16B
CODE B-1
CODE B-2
10C
TRANSMITTER
ENCODER
16C
CODE C-1
CODE C-2
12
RECEIVER
14
CONTROL UNIT
14A
CONTROL UNIT MEMORY

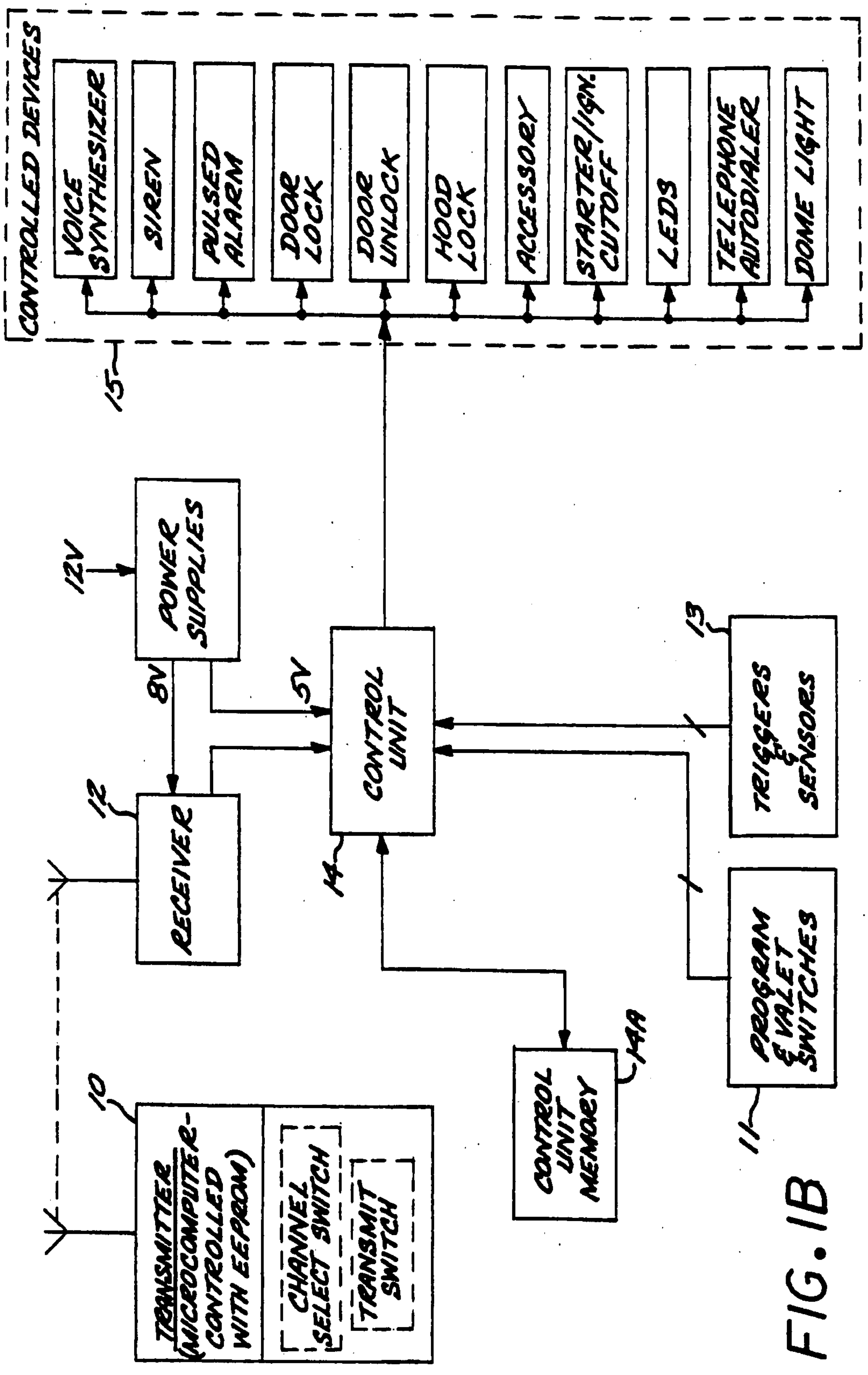

CONTROLLED DEVICES
VOICE SYNTHESIZER
SIREN
PULSED ALARM
DOOR LOCK
DOOR UNLOCK
HOOD LOCK
ACCESSORY
STARTER/IGN. CUTOFF
LEDS
TELEPHONE AUTODIALER
DOME LIGHT
15
12V
POWER SUPPLIES
8V
5V
CONTROL UNIT
13
TRIGGERS & SENSORS
12
RECEIVER
14
PROGRAM & VALET SWITCHES
14A
CONTROL UNIT MEMORY
11
10
TRANSMITTER (MICROCOMPUTER-CONTROLLED WITH EEPROM)
CHANNEL SELECT SWITCH
TRANSMIT SWITCH

FIG. 1B

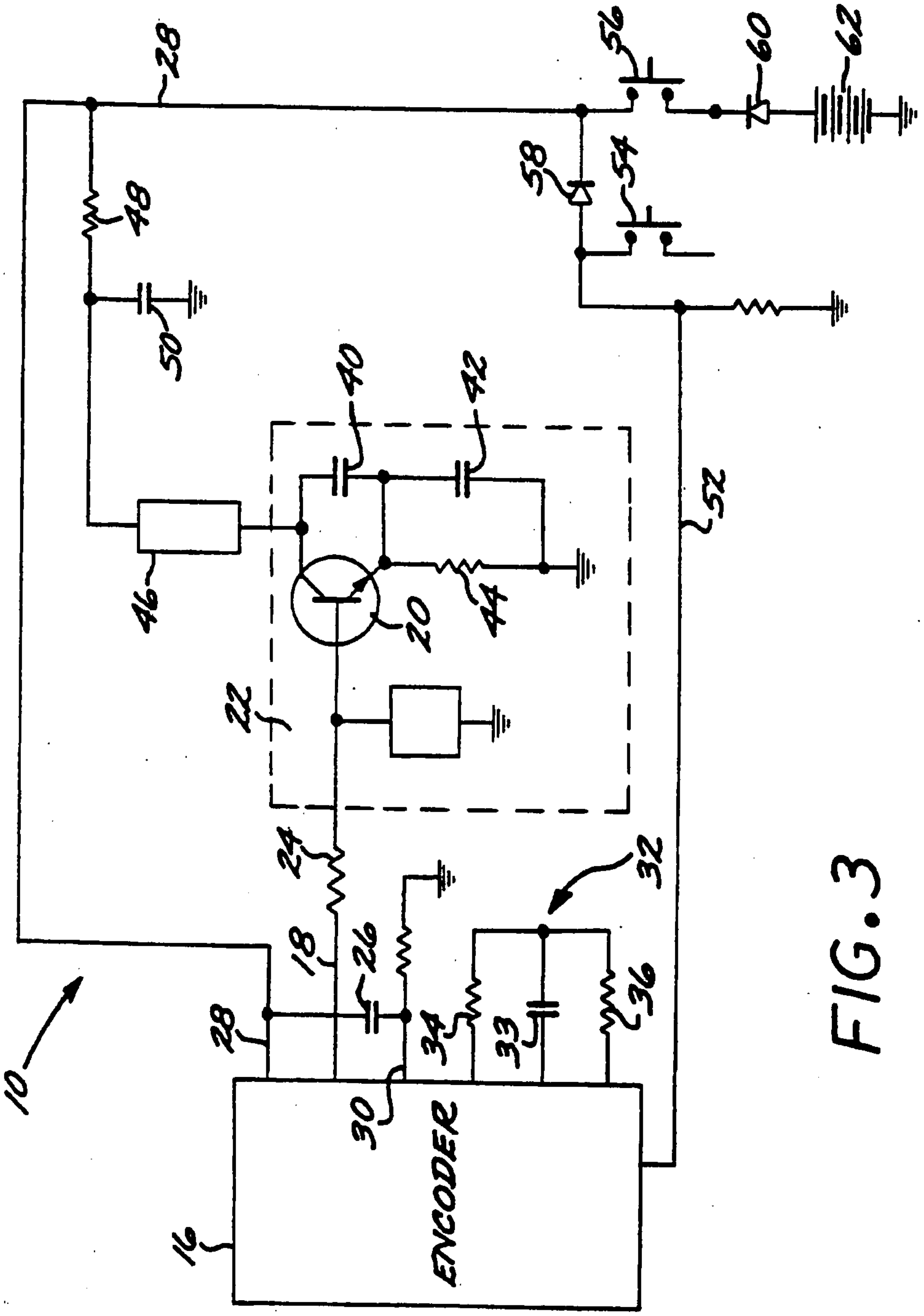

ENCODER
10
16
18
20
22
24
26
28
30
32
33
34
36
40
42
44
46
48
50
52
54
56
58
60
62

FIG. 3

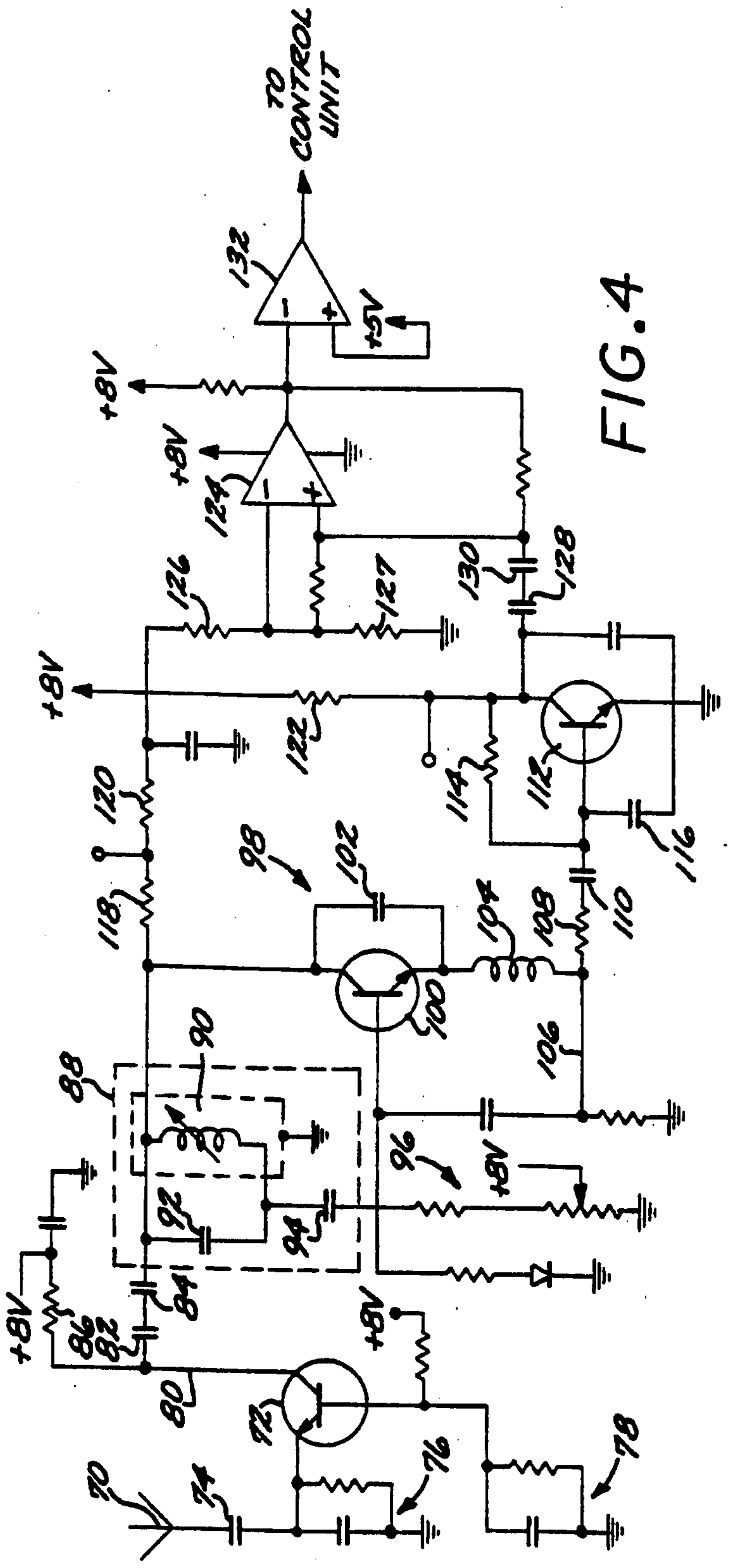

TO CONTROL UNIT
+8V
+5V
132
124
126
127
128
130
122
120
118
114
112
116
110
108
106
104
102
100
98
96
94
92
90
88
86
84
82
80
78
76
74
72
70

FIG. 4

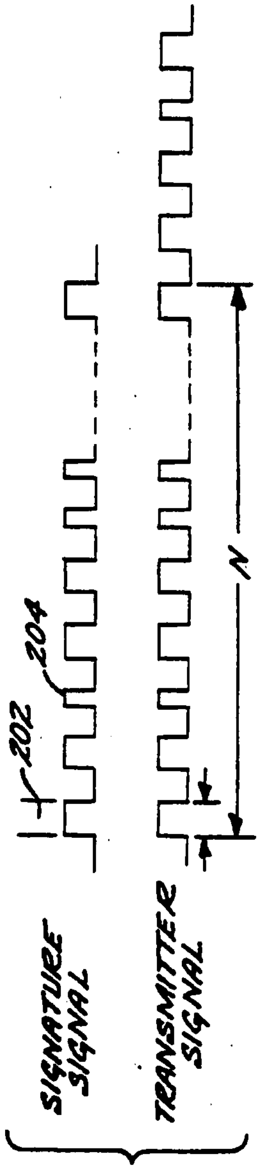

SIGNATURE SIGNAL
TRANSMITTER SIGNAL
202
204
N

FIG. 6

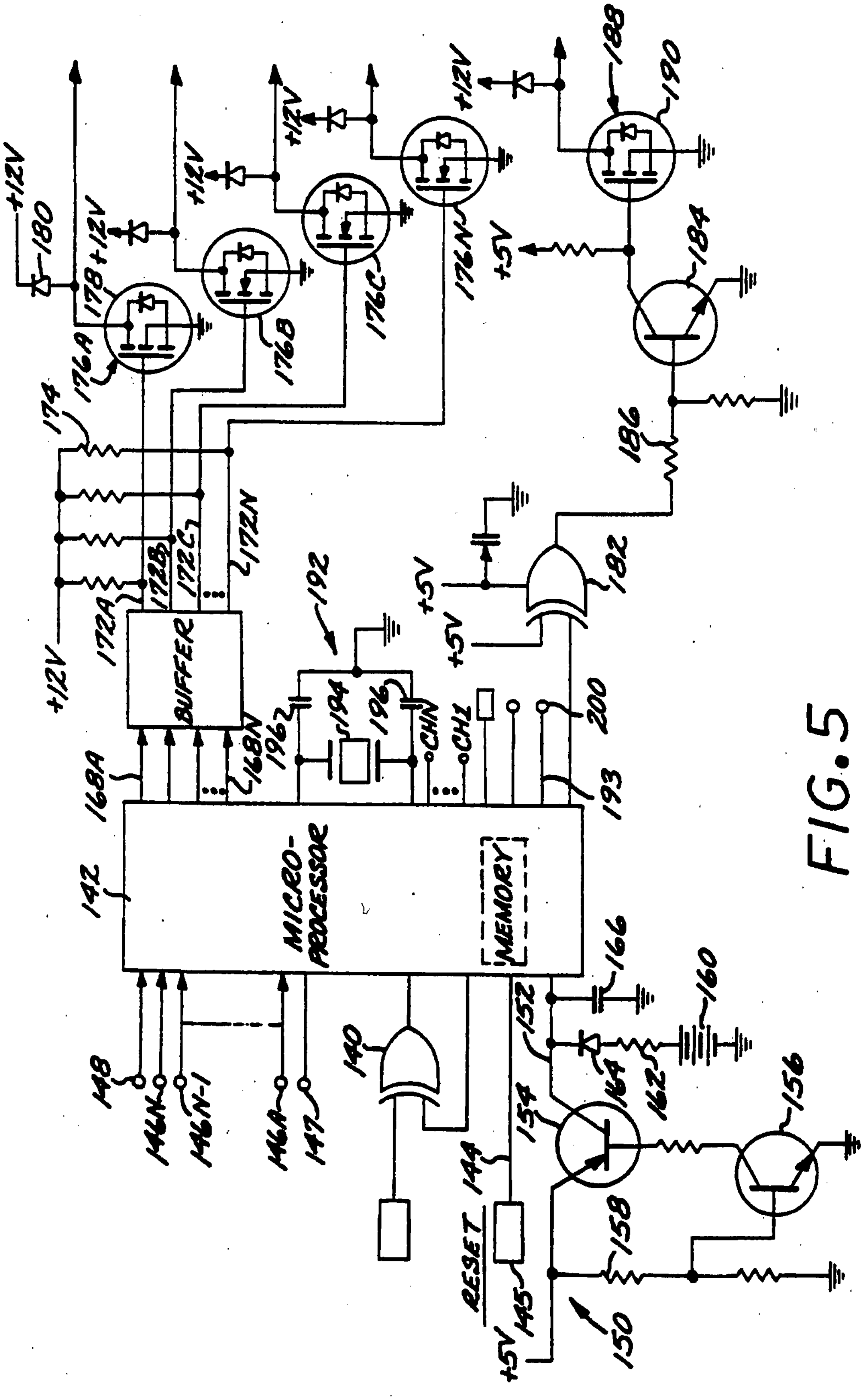

MICRO-PROCESSOR
MEMORY
BUFFER
RESET
+12V
+5V
CHN
CH1
142
140
144
145
146A
146N
146N-1
147
148
150
152
154
156
158
160
162
164
166
168A
168N
172A
172B
172C
172N
174
176A
176B
176C
176N
178
180
182
184
186
188
190
192
193
194
196
200

FIG. 5

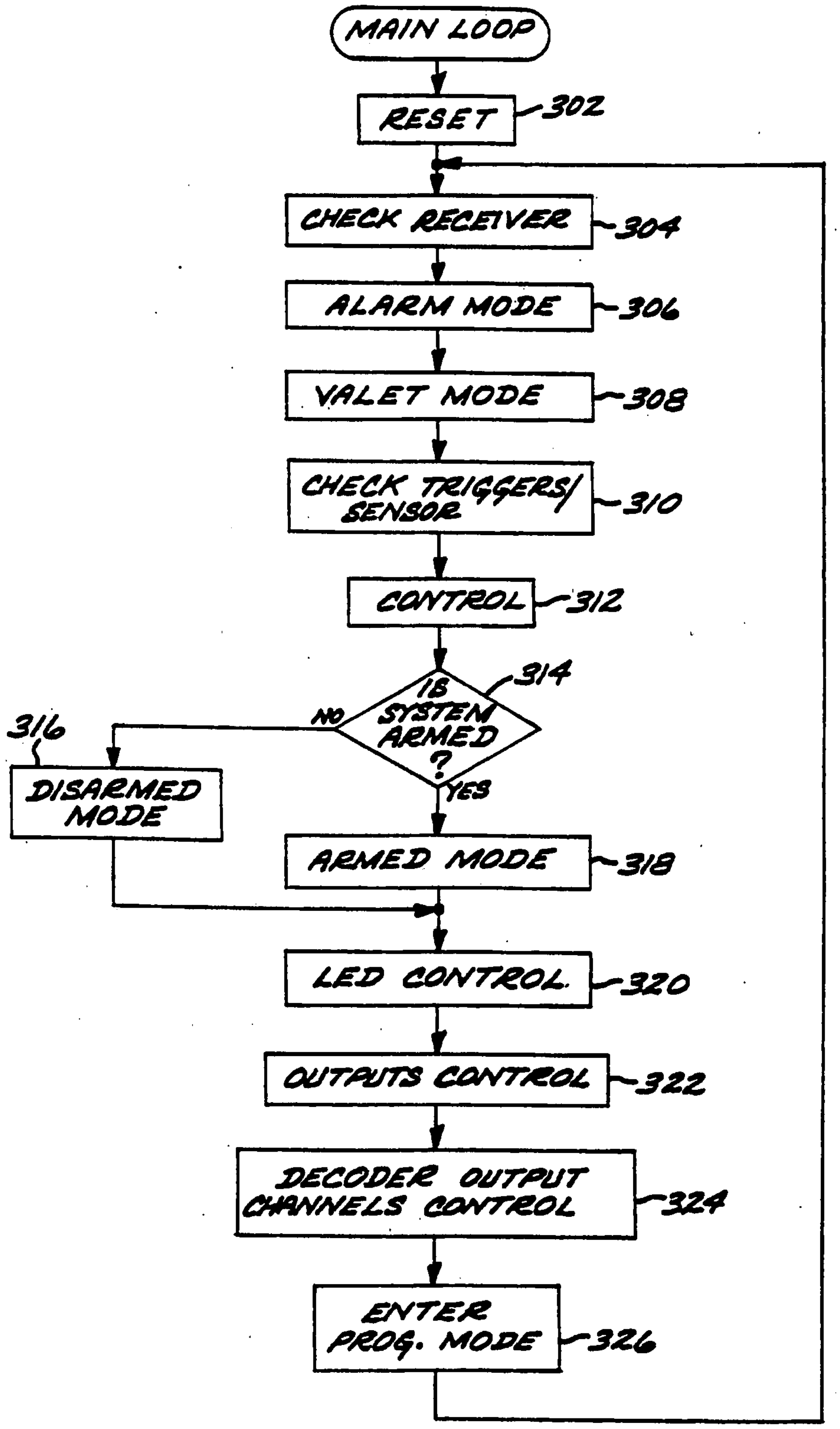

MAIN LOOP
RESET
302
CHECK RECEIVER
304
ALARM MODE
306
VALET MODE
308
CHECK TRIGGERS/ SENSOR
310
CONTROL
312
IS SYSTEM ARMED ?
314
NO
YES
316
DISARMED MODE
ARMED MODE
318
LED CONTROL
320
OUTPUTS CONTROL
322
DECODER OUTPUT CHANNELS CONTROL
324
ENTER PROG. MODE
326

FIG. 7

FIG. 8

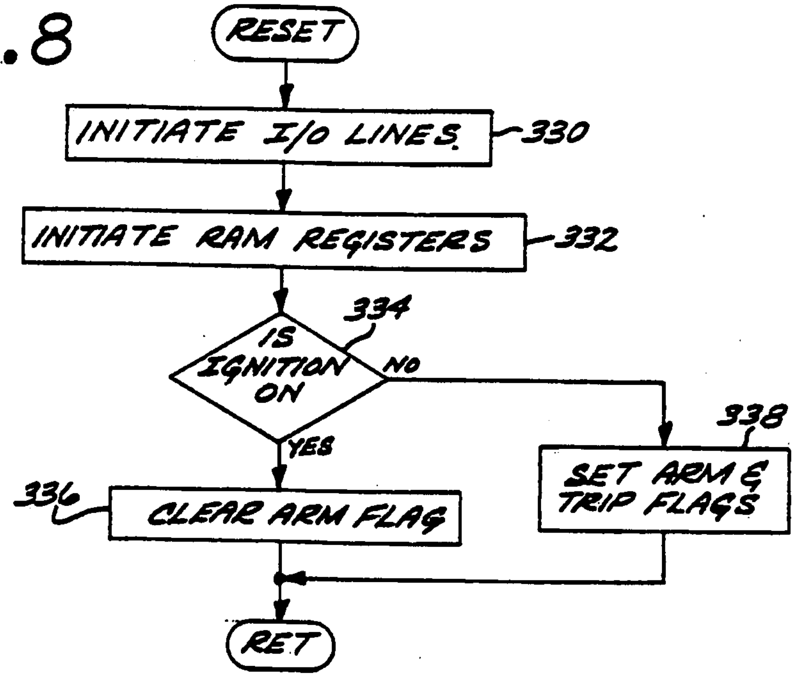
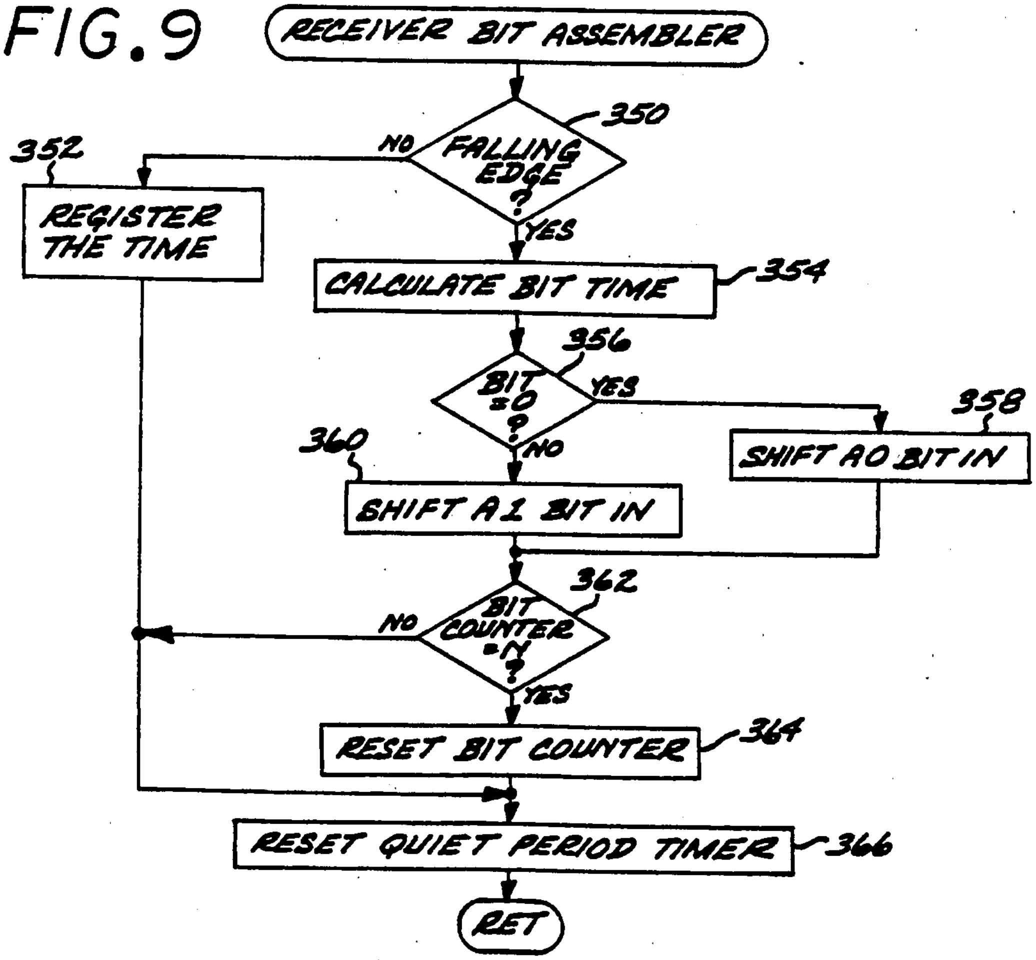

RESET
INITIATE I/O LINES
330
INITIATE RAM REGISTERS
332
IS IGNITION ON
334
NO
YES
338
SET ARM & TRIP FLAGS
336
CLEAR ARM FLAG
RET

FIG. 9


RECEIVER BIT ASSEMBLER
FALLING EDGE ?
350
NO
YES
352
REGISTER THE TIME
CALCULATE BIT TIME
354
BIT =0 ?
356
YES
NO
358
SHIFT A0 BIT IN
360
SHIFT A1 BIT IN
BIT COUNTER =N ?
362
NO
YES
RESET BIT COUNTER
364
RESET QUIET PERIOD TIMER
366
RET

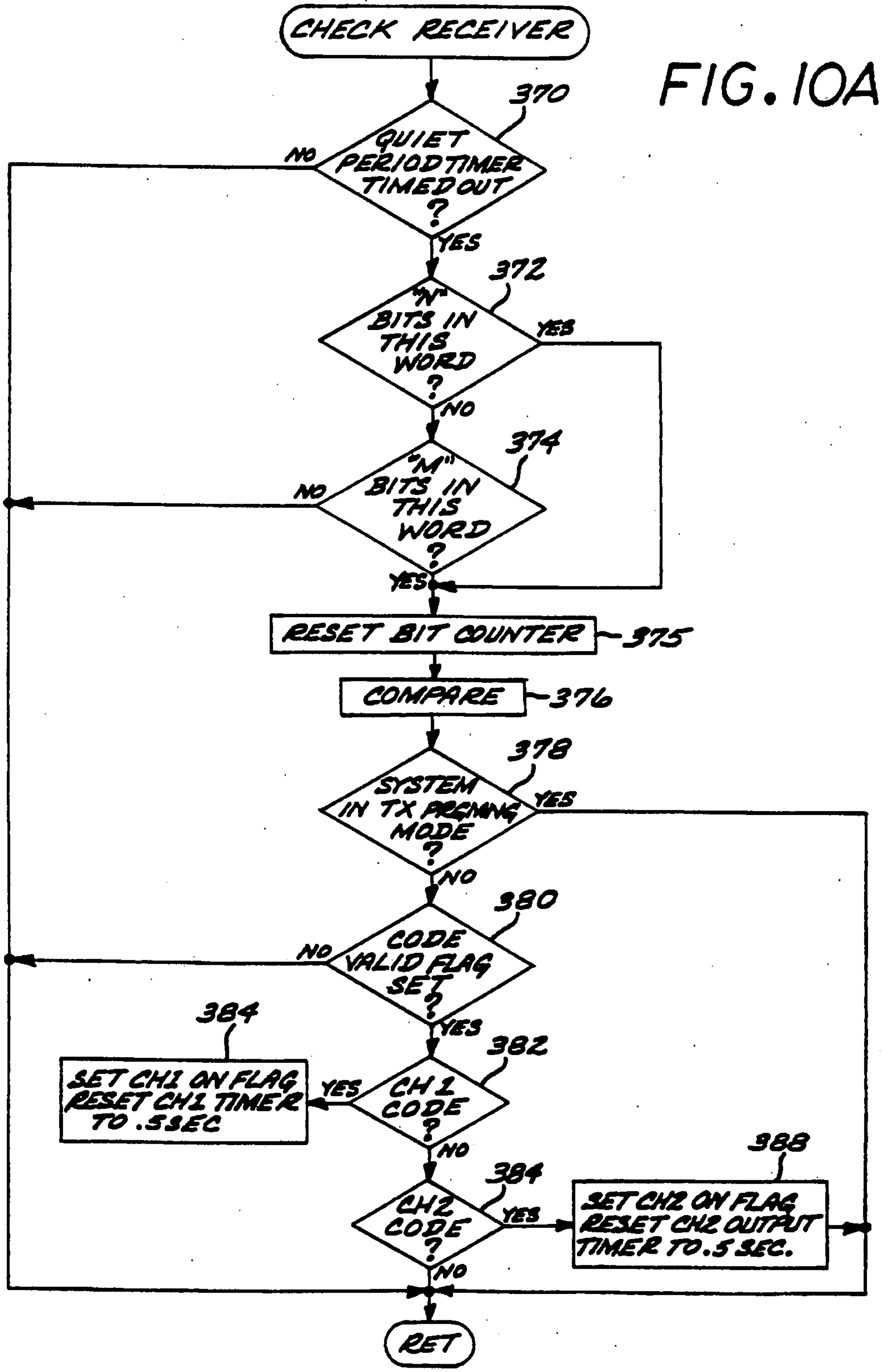
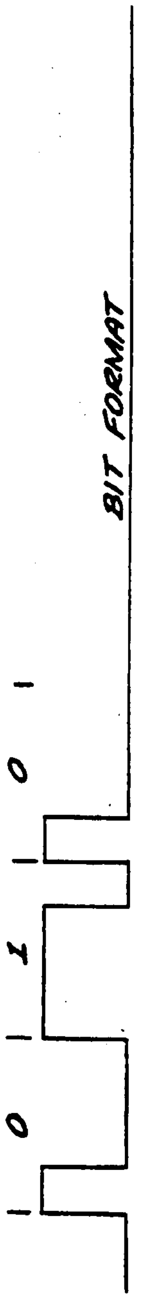
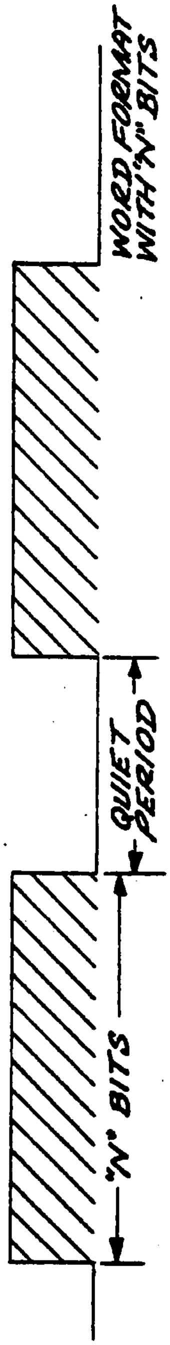

CHECK RECEIVER
370
QUIET PERIOD TIMER TIMED OUT ?
NO
YES
372
"N" BITS IN THIS WORD ?
YES
NO
374
"M" BITS IN THIS WORD ?
NO
YES
RESET BIT COUNTER
375
COMPARE
376
378
SYSTEM IN TX PRGMING MODE ?
YES
NO
380
CODE VALID FLAG SET ?
NO
YES
384
SET CH1 ON FLAG RESET CH1 TIMER TO .5SEC
YES
382
CH1 CODE ?
NO
384
388
CH2 CODE ?
YES
SET CH2 ON FLAG RESET CH2 OUTPUT TIMER TO .5 SEC.
NO
RET

FIG. 10A



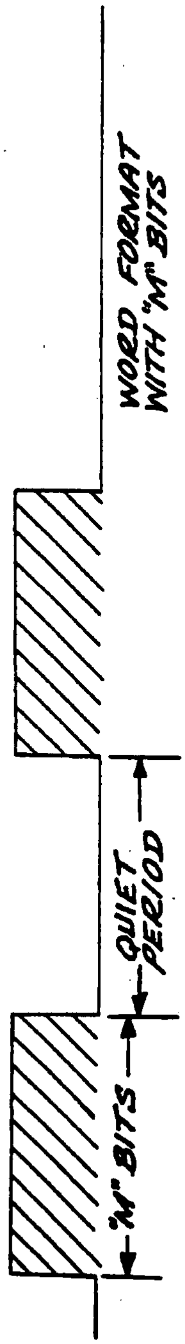
BIT FORMAT
0
1
0

FIG. 10B



WORD FORMAT WITH "N" BITS
QUIET PERIOD
"N" BITS

FIG. 10C



WORD FORMAT WITH "M" BITS
QUIET PERIOD
"M" BITS

FIG. 10D

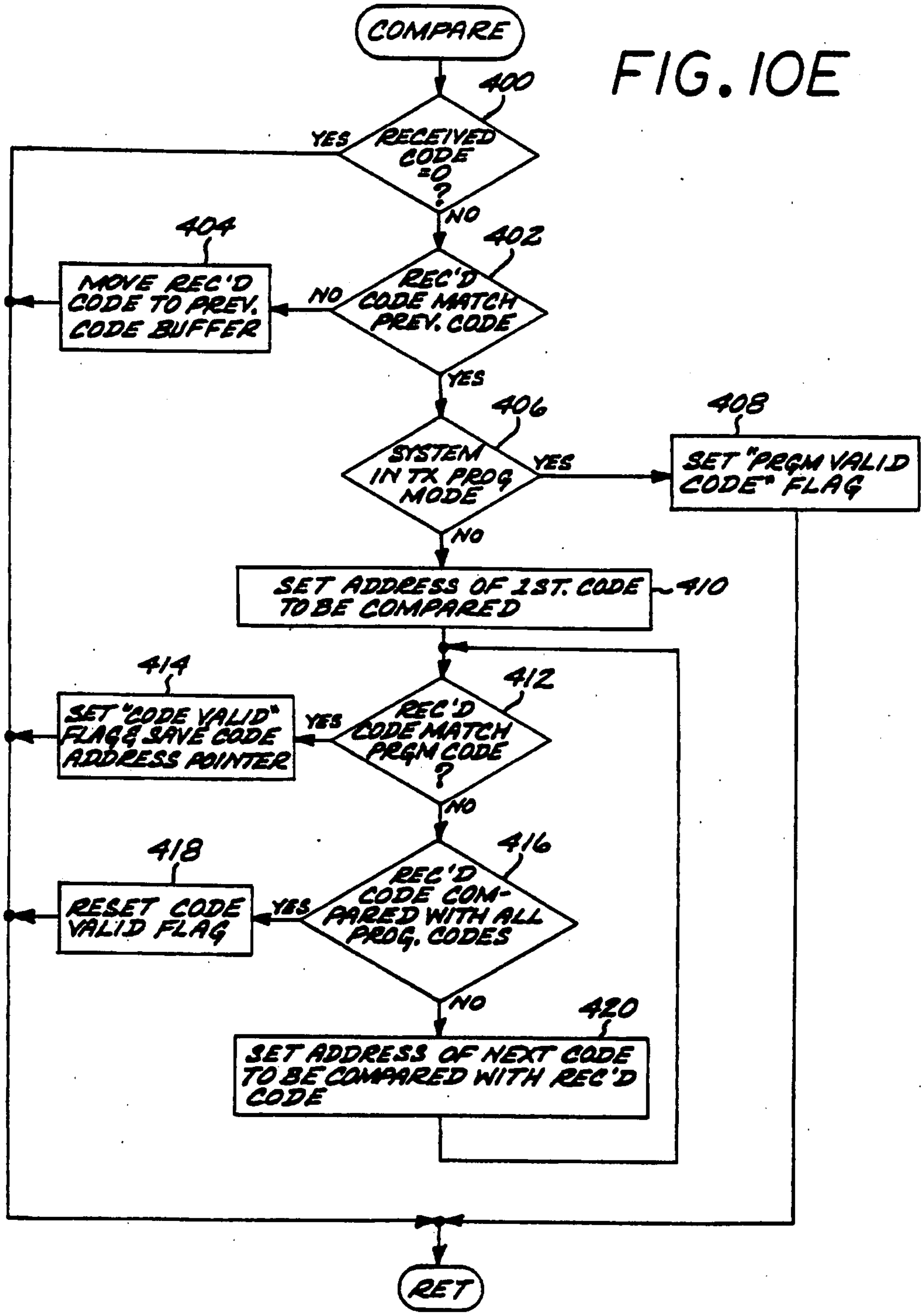

COMPARE
400
RECEIVED CODE =0 ?
YES
NO
402
REC'D CODE MATCH PREV. CODE
404
MOVE REC'D CODE TO PREV. CODE BUFFER
NO
YES
406
SYSTEM IN TX PROG MODE
YES
408
SET "PRGM VALID CODE" FLAG
NO
SET ADDRESS OF 1ST. CODE TO BE COMPARED
410
412
REC'D CODE MATCH PRGM CODE ?
YES
414
SET "CODE VALID" FLAG & SAVE CODE ADDRESS POINTER
NO
416
REC'D CODE COMPARED WITH ALL PROG. CODES
YES
418
RESET CODE VALID FLAG
NO
420
SET ADDRESS OF NEXT CODE TO BE COMPARED WITH REC'D CODE
RET

FIG. 10E

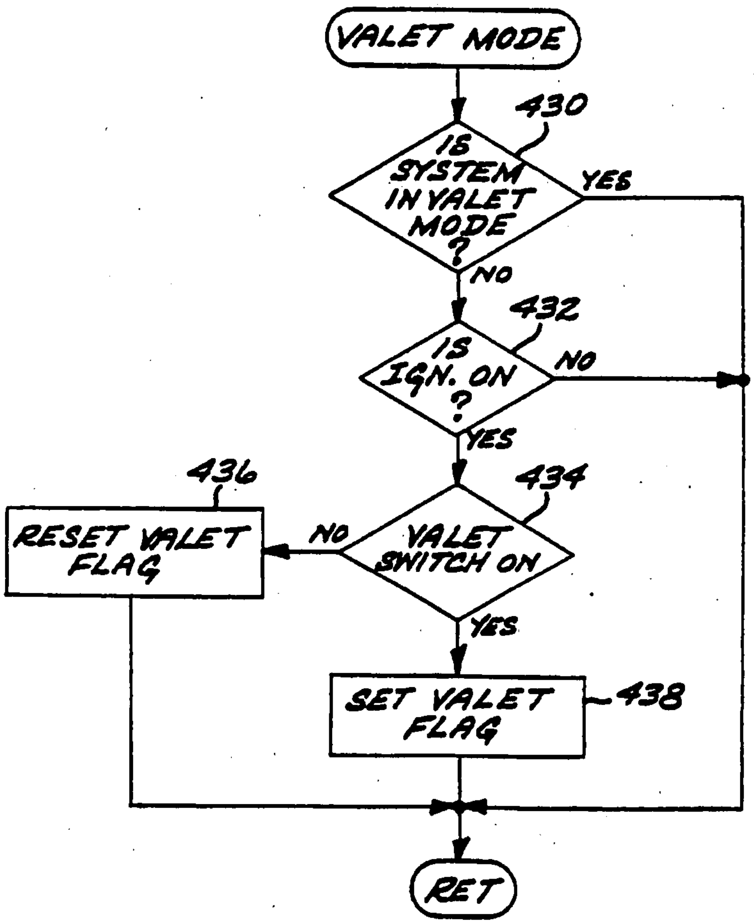

VALET MODE
430
IS SYSTEM IN VALET MODE ?
YES
NO
432
IS IGN. ON ?
NO
YES
434
VALET SWITCH ON
NO
YES
436
RESET VALET FLAG
SET VALET FLAG
438
RET

FIG. 11

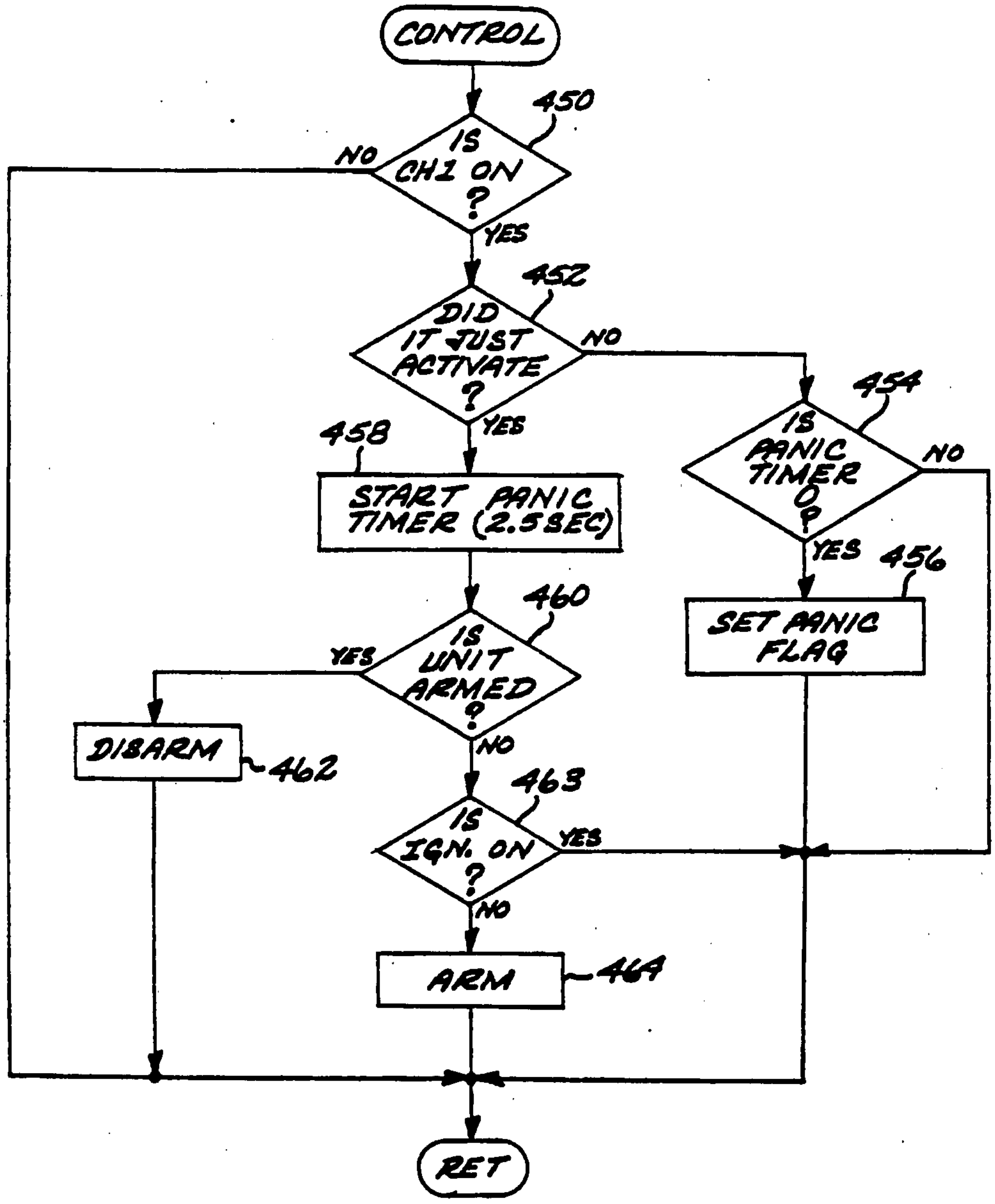

CONTROL
450
IS CH1 ON ?
NO
YES
452
DID IT JUST ACTIVATE ?
NO
YES
458
START PANIC TIMER (2.5SEC)
454
IS PANIC TIMER 0 ?
NO
YES
456
SET PANIC FLAG
460
IS UNIT ARMED ?
YES
NO
DISARM
462
463
IS IGN. ON ?
YES
NO
ARM
464
RET

FIG. 12

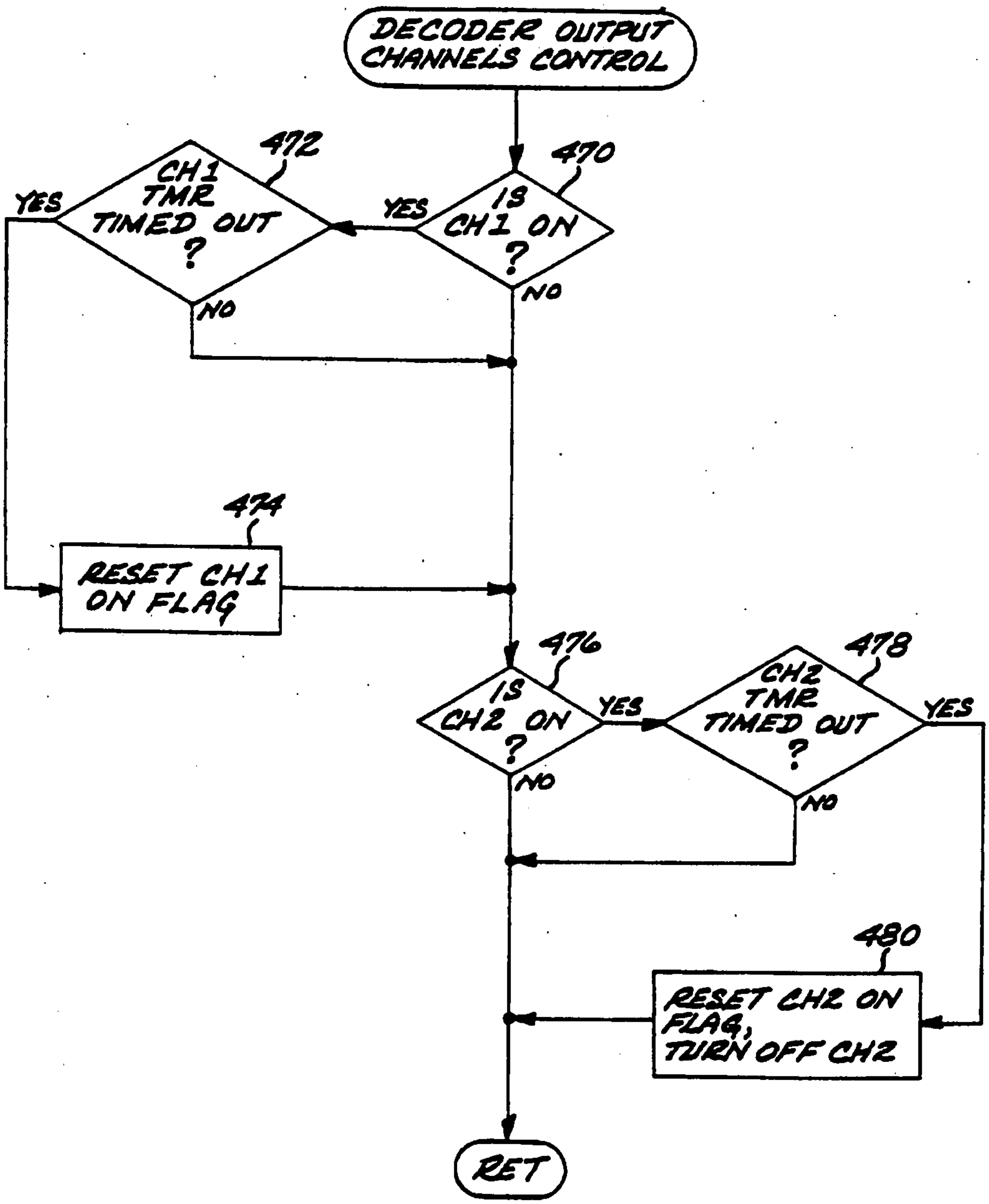

DECODER OUTPUT CHANNELS CONTROL
470
IS CH1 ON ?
YES
NO
472
CH1 TMR TIMED OUT ?
YES
NO
474
RESET CH1 ON FLAG
476
IS CH2 ON ?
YES
NO
478
CH2 TMR TIMED OUT ?
YES
NO
480
RESET CH2 ON FLAG, TURN OFF CH2
RET

FIG. 13

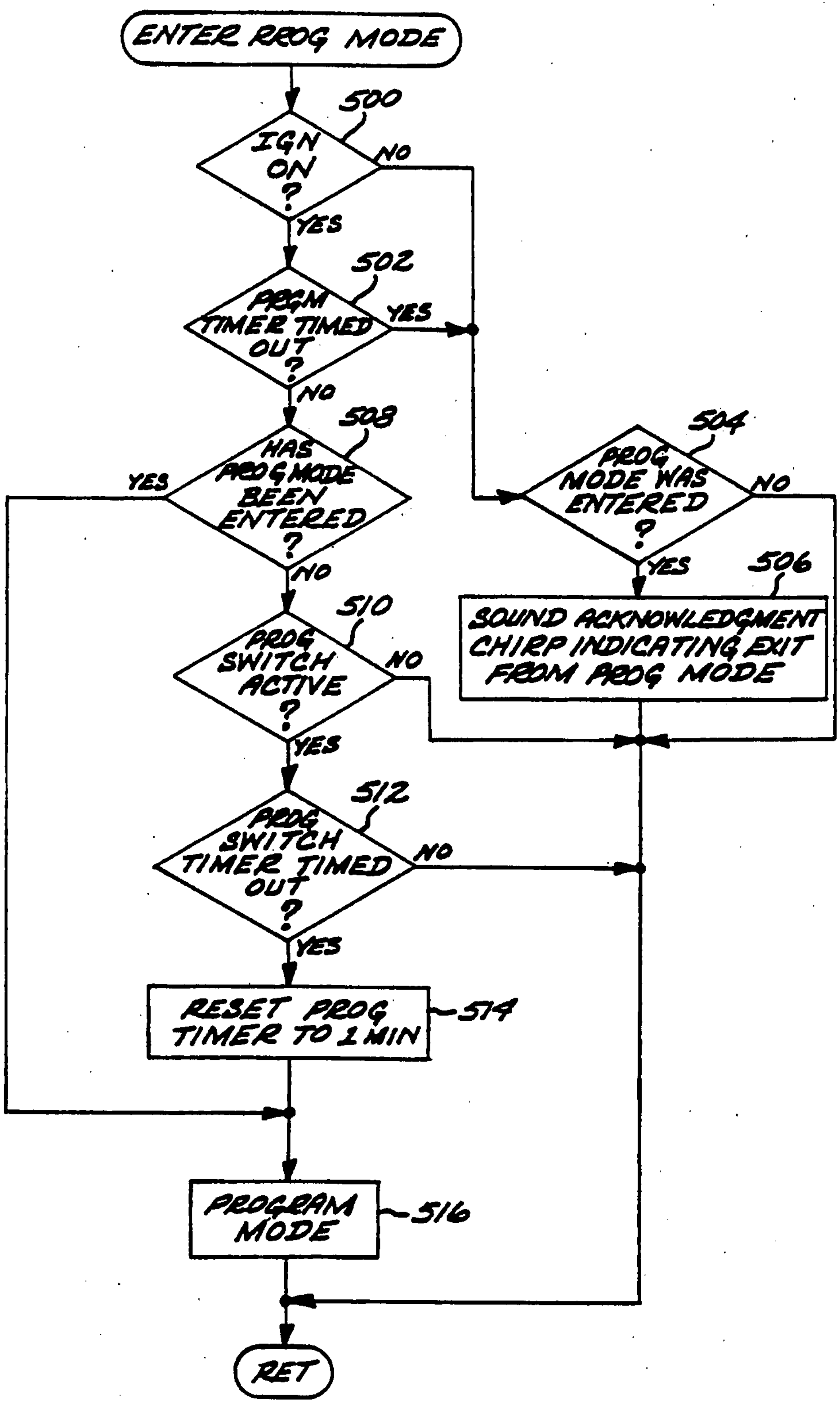

ENTER PROG MODE
500
IGN ON ?
NO
YES
502
PRGM TIMER TIMED OUT ?
YES
NO
508
HAS PROG MODE BEEN ENTERED ?
YES
NO
504
PROG MODE WAS ENTERED ?
NO
YES
506
SOUND ACKNOWLEDGMENT CHIRP INDICATING EXIT FROM PROG MODE
510
PROG SWITCH ACTIVE ?
NO
YES
512
PROG SWITCH TIMER TIMED OUT ?
NO
YES
RESET PROG TIMER TO 1 MIN
514
PROGRAM MODE
516
RET

FIG. 14

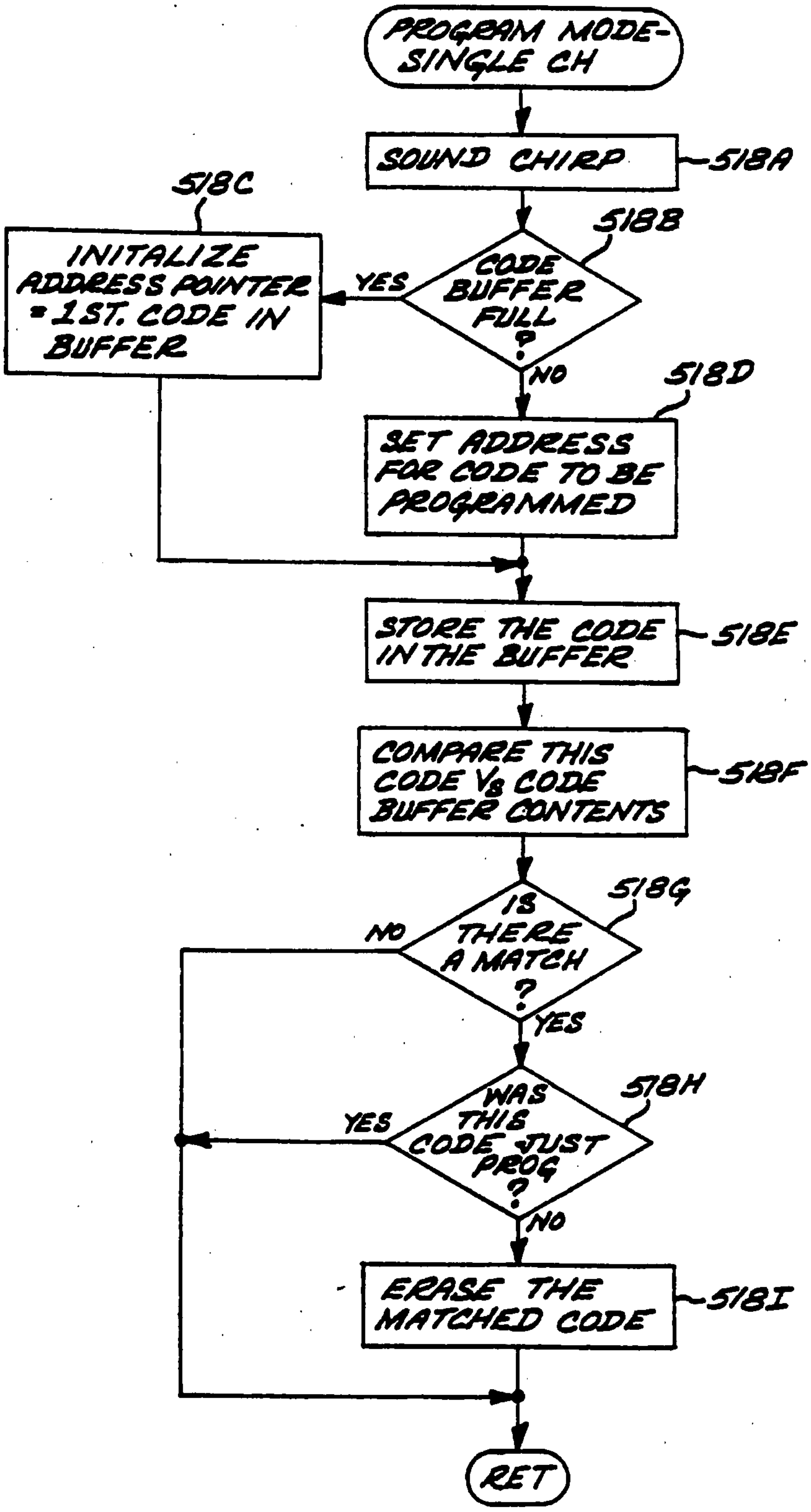

PROGRAM MODE-SINGLE CH
SOUND CHIRP
518A
518C
518B
INITALIZE ADDRESS POINTER =1ST. CODE IN BUFFER
YES
CODE BUFFER FULL ?
NO
518D
SET ADDRESS FOR CODE TO BE PROGRAMMED
STORE THE CODE IN THE BUFFER
518E
COMPARE THIS CODE Vs CODE BUFFER CONTENTS
518F
518G
NO
IS THERE A MATCH ?
YES
518H
YES
WAS THIS CODE JUST PROG ?
NO
ERASE THE MATCHED CODE
518I
RET

FIG. 15

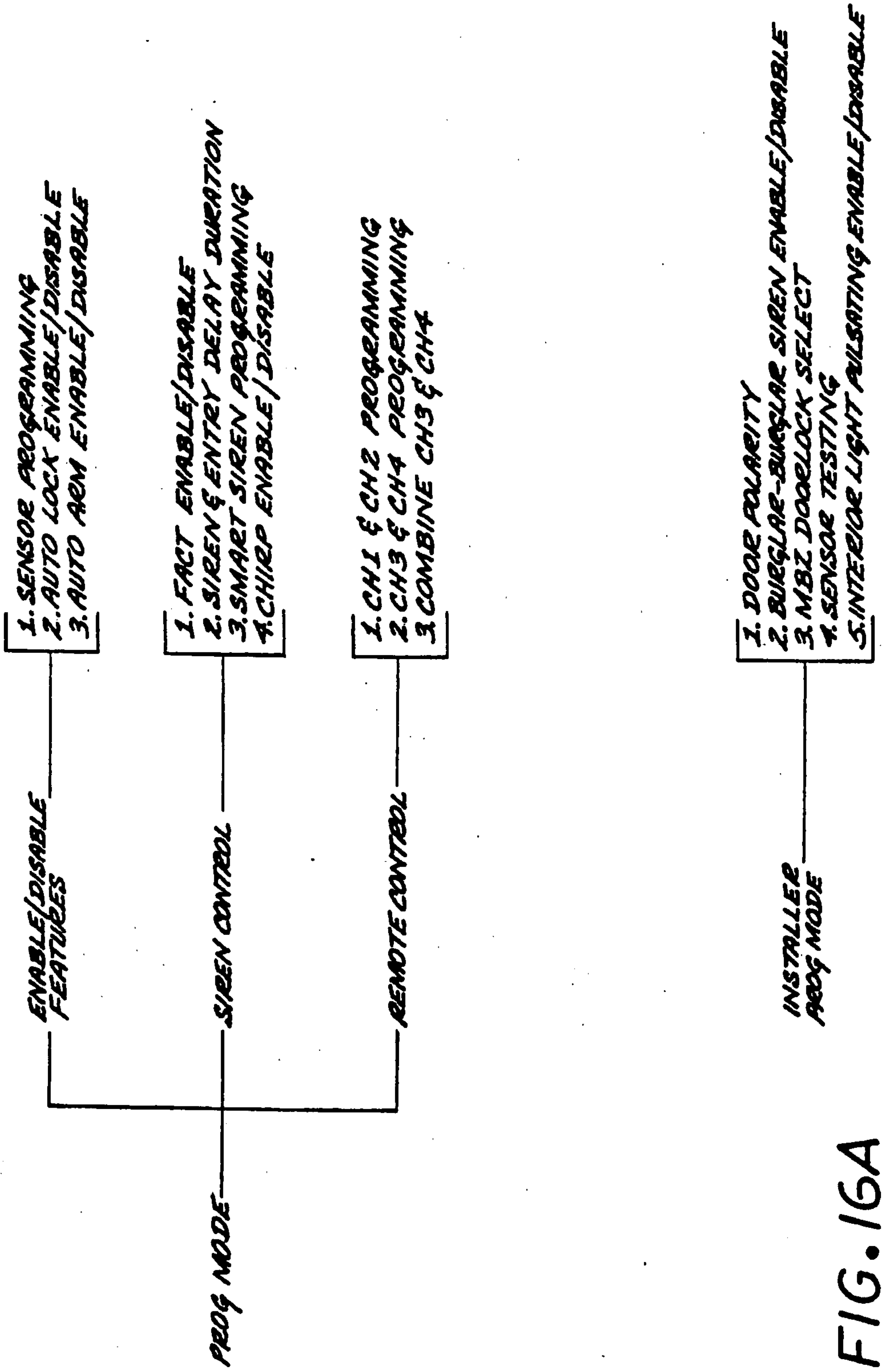
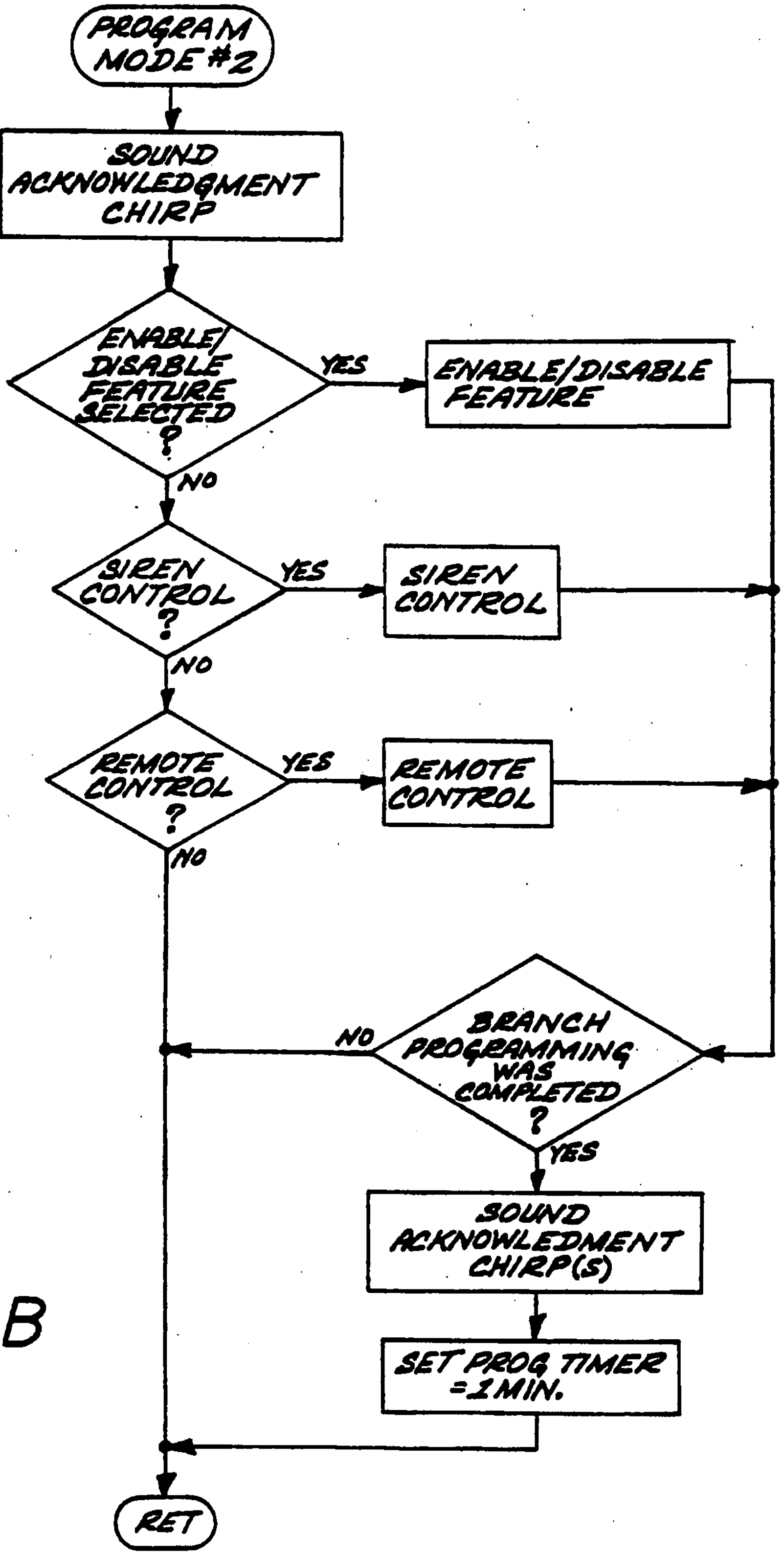
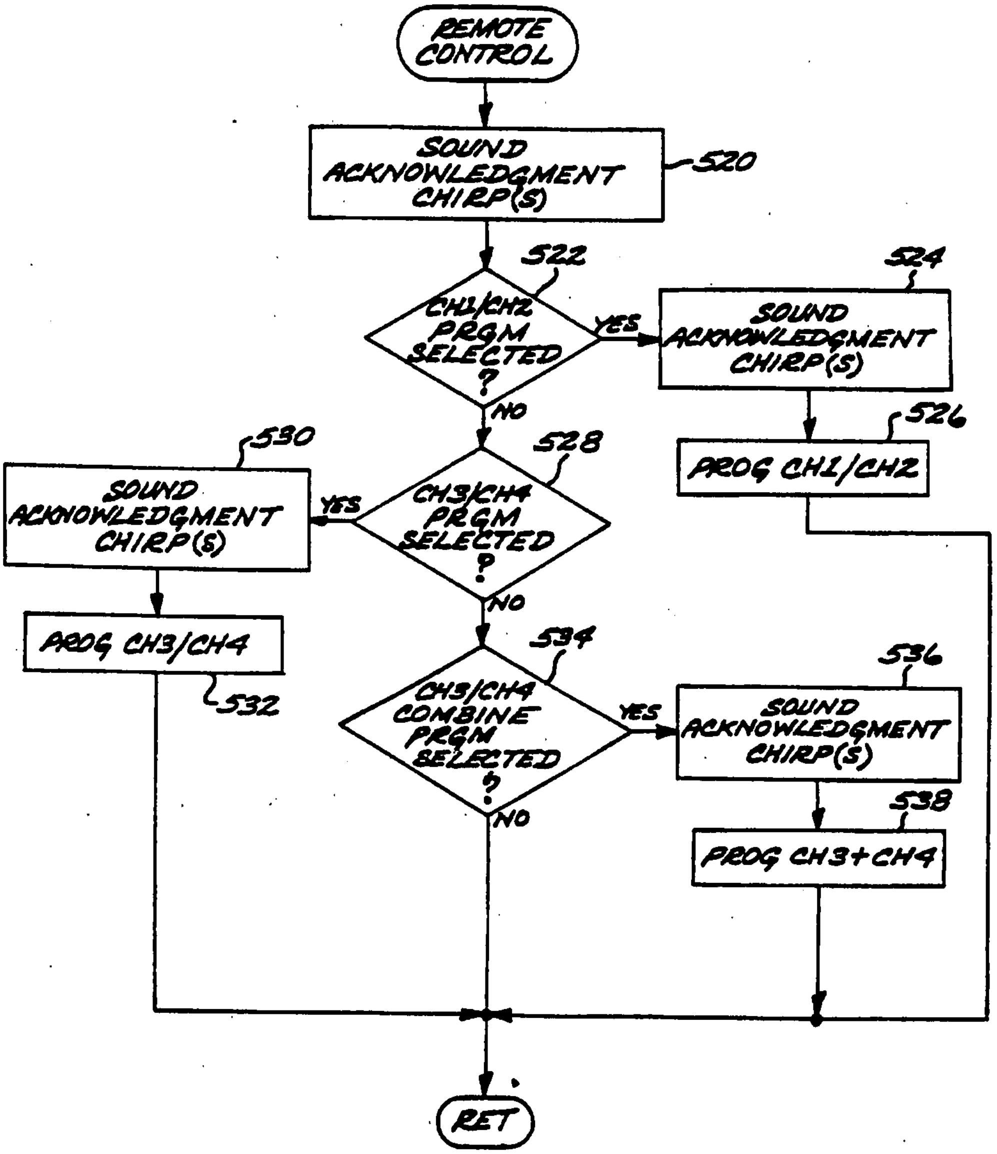

PROG MODE
ENABLE/DISABLE FEATURES
1. SENSOR PROGRAMMING
2. AUTO LOCK ENABLE/DISABLE
3. AUTO ARM ENABLE/DISABLE
SIREN CONTROL
1. FACT ENABLE/DISABLE
2. SIREN & ENTRY DELAY DURATION
3. SMART SIREN PROGRAMMING
4. CHIRP ENABLE/DISABLE
REMOTE CONTROL
1. CH1 & CH2 PROGRAMMING
2. CH3 & CH4 PROGRAMMING
3. COMBINE CH3 & CH4
INSTALLER PROG MODE
1. DOOR POLARITY
2. BURGLAR-BURGLAR SIREN ENABLE/DISABLE
3. MBZ DOORLOCK SELECT
4. SENSOR TESTING
5. INTERIOR LIGHT PULSATING ENABLE/DISABLE

FIG. 16A



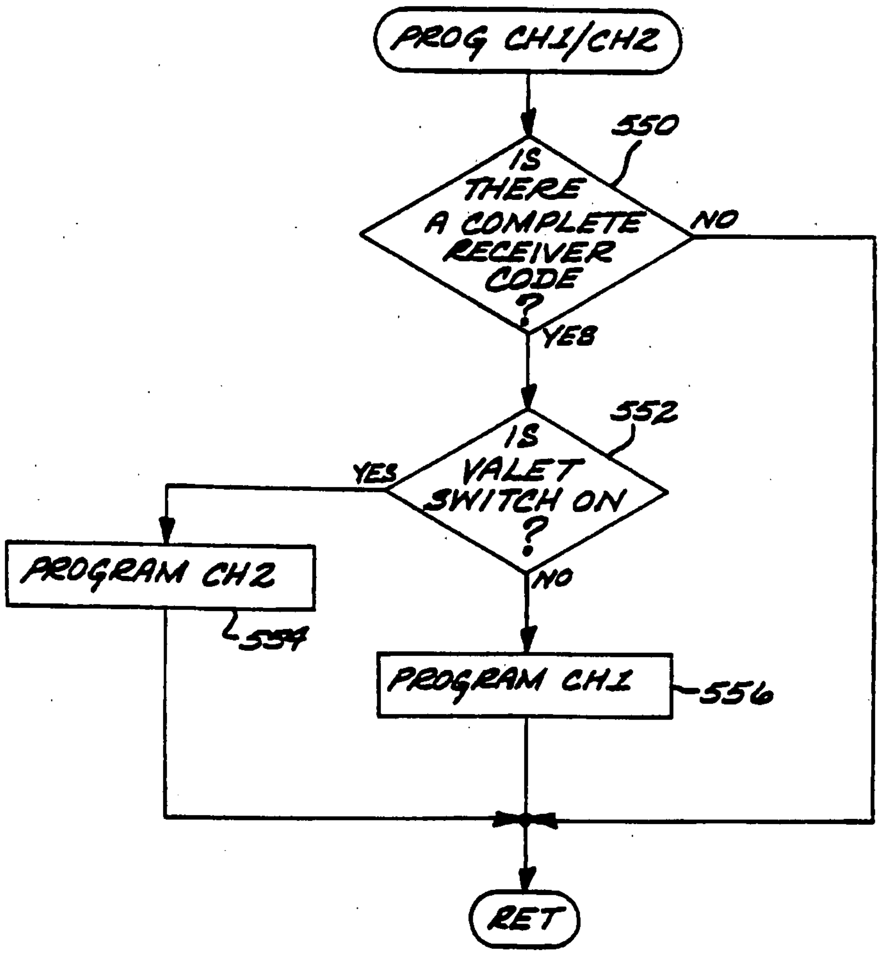
PROGRAM MODE #2
SOUND ACKNOWLEDGMENT CHIRP
ENABLE/ DISABLE FEATURE SELECTED ?
YES
ENABLE/DISABLE FEATURE
NO
SIREN CONTROL ?
YES
SIREN CONTROL
NO
REMOTE CONTROL ?
YES
REMOTE CONTROL
NO
BRANCH PROGRAMMING WAS COMPLETED ?
NO
YES
SOUND ACKNOWLEDMENT CHIRP(S)
SET PROG TIMER =1 MIN.
RET

FIG.16B



REMOTE CONTROL
SOUND ACKNOWLEDGMENT CHIRP(S)
520
522
CH1/CH2 PRGM SELECTED ?
YES
NO
524
SOUND ACKNOWLEDGMENT CHIRP(S)
526
PROG CH1/CH2
530
SOUND ACKNOWLEDGMENT CHIRP(S)
YES
528
CH3/CH4 PRGM SELECTED ?
NO
PROG CH3/CH4
532
534
CH3/CH4 COMBINE PRGM SELECTED ?
YES
NO
536
SOUND ACKNOWLEDGMENT CHIRP(S)
538
PROG CH3+CH4
RET

FIG. 16C



PROG CH1/CH2
550
IS THERE A COMPLETE RECEIVER CODE ?
NO
YES
552
IS VALET SWITCH ON ?
YES
PROGRAM CH2
554
NO
PROGRAM CH1
556
RET

FIG. 16D

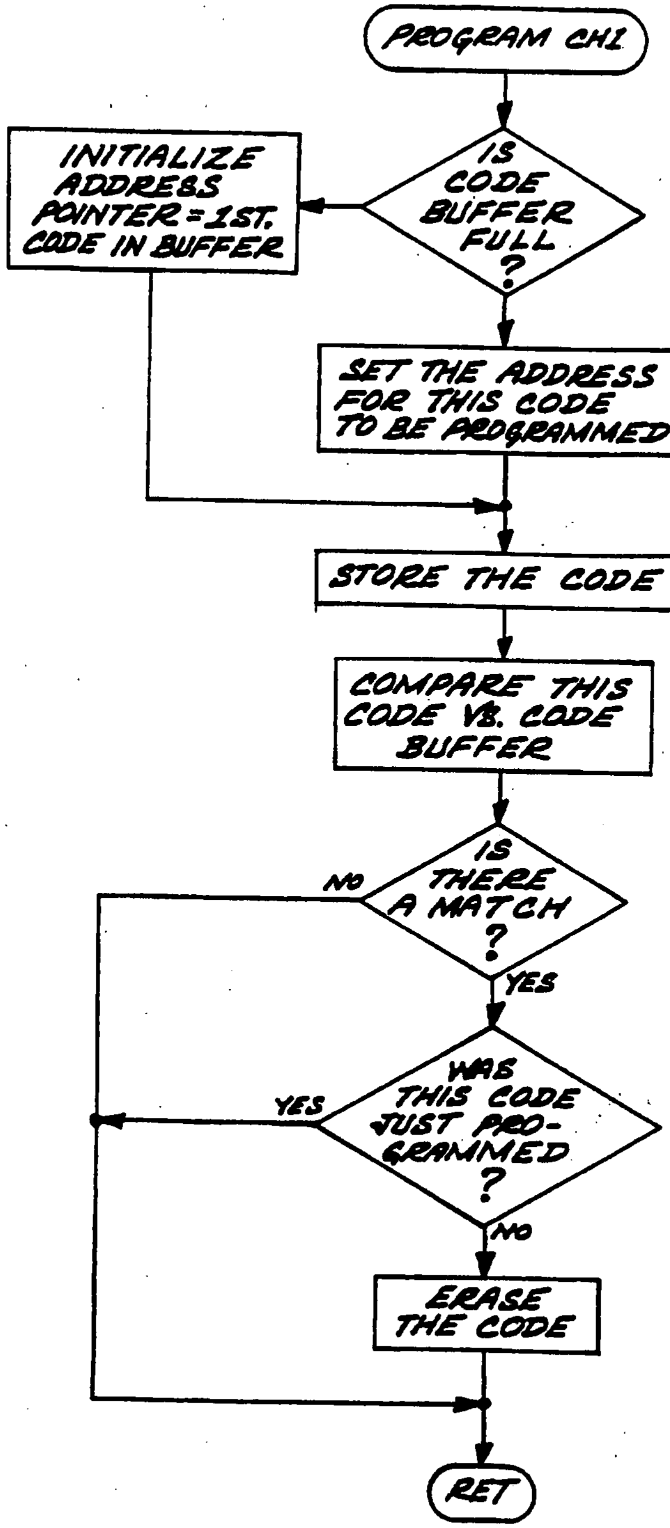

PROGRAM CH1
IS CODE BUFFER FULL ?
INITIALIZE ADDRESS POINTER=1ST. CODE IN BUFFER
SET THE ADDRESS FOR THIS CODE TO BE PROGRAMMED
STORE THE CODE
COMPARE THIS CODE VS. CODE BUFFER
IS THERE A MATCH ?
NO
YES
WAS THIS CODE JUST PRO-GRAMMED ?
YES
NO
ERASE THE CODE
RET

FIG. 16E

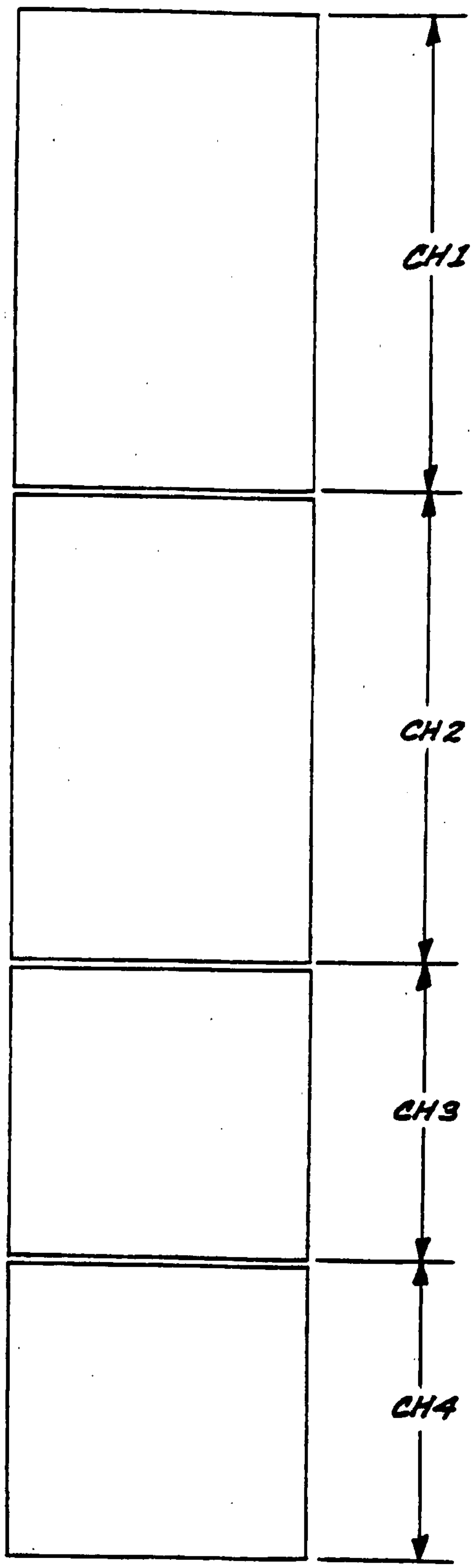

CH1
CH2
CH3
CH4

FIG. 16F

ELECTRONICALLY PROGRAMMABLE REMOTE CONTROL FOR VEHICLE SECURITY SYSTEM

This is a continuation-in-pat of application Ser. No. 07/094,395, filed Sep. 8, 1987, now abandoned. Also this application is a continuation-in-part of application Ser. No. 07/231,159, filed Aug. 11, 1988, now U.S. Pat. No. 4,922,224.

BACKGROUND OF THE INVENTION

This invention relates to certain new and useful improvements in remote control vehicle security systems, and more particularly, to remote control vehicle security systems including a receiver-control unit located in the vehicle, and one or more remote transmitters, and which systems are electronically programmable by the user without knowledge of the specific transmitter code.

In recent years, primarily due to the increase of theft, vandalism and burglaries, many vehicle owners have installed remote control security systems. The vast majority of these security systems, when triggered, will generate an audible or visible alarm signal to alert of an improper entry or intrusion into the vehicle. Many of these commercially available security systems are remotely operable, that is, they include a receiver capable of being operated from a remotely located transmitter for purposes of arming and disarming the security system. Usually, these receiver-transmitter arrangements are radio frequency operated, although they can be operated with other forms of electromagnetic radiation or sound energy.

Automotive vehicle security systems known in the art usually include an alarm section which may either generate an audible alarm, as for example, from a siren, a horn, or the like and may also often activate a visible alarm by operating any of the vehicle lights. Many of these commercially available vehicle security systems may also disable some portion of the vehicle engine system such as the ignition system, starter, fuel pump, or lock the engine compartment. Thus, in the event of an improper intrusion or attempted theft of the vehicle, the security system will cause initiation of an audible alarm or cause the lights to switch on and off and may also interfere with operation of the vehicle engine system. One example of a remote control vehicle security system is disclosed in U.S. pat. No. 4,383,242.

The use of a transmitter and a receiver which have been precoded is generally standard with commercially available remote control vehicle security systems. In these conventional transmitter-receiver combinations, the code, usually referred to as an encoded signal, is permanently encoded into the receiver, and the transmitters is preprogrammed with a code which cannot be altered or changed by the user. Thus, the receiver is operated on the basis of a security code permanently encoded in that receiver and transmitted from a particular transmitter matched and sold with that receiver. Such conventional security systems present a security exposure in case of a lost or stolen transmitter, as well as many constraints on the manufacturers, customers and dealers of these security systems. For instance, if the user of one of these security systems should lose the transmitter, it is necessary to obtain another transmitter which was not previously coded and have that transmitter properly matched and coded for the particular receiver.

The encoding of the transmitter entails obtaining the particular code required to activate the receiver, opening the transmitter housing and mechanically coding the transmitter. Usually, the coding is accomplished by scratching conductive lines on a printed circuit board, closing or opening switches or the like. Some transmitters are provided with control boards having hole areas capable of being punched to provide a particular encoded signal. Thus, some form of mechanical action is usually required for encoding the transmitter.

Most users of remote control vehicle security systems do not have the expertise to encode the transmitter and, therefore, must seek the assistance of the retailer or manufacturer of the system. The mere fact that the code for authorized actuation of the security system must be known by the selling dealer or manufacturer may inevitably lead to a breach of the security system itself, since the code is usually written to maintain a permanent record of the same. More importantly, should the user wish to change the code because of a lost or stolen transmitter, the receiver will have to be sent back to the manufacturer, leaving the user without the security system while this costly task is being performed.

In addition to the foregoing, if a user desires to have several transmitters operate the receivers of several remote control vehicle security systems, each receiver must be properly programmed with the proper code. Thus, if a person desired to operate several vehicles with the same remote control system, it is necessary to have a receiver in each car preprogrammed by a manufacturer. This necessarily requires custom design efforts which is very time consuming as well as costly.

It is, therefore, one of the primary objects of the present invention to provide a radio frequency operated remote control vehicle security system in which the receiver of the system can be electronically programmed by the user of the system without opening the transmitter, and without coding the transmitter or changing or encoding the receiver or acquiring dealer or manufacturer assistance.

It is another object of the present invention to provide a remote control vehicle security system in which neither the manufacturer, dealer or user of the system is required to know the particular code which is transmitted from the transmitter to the receiver.

It is a further object of the present invention to provide a method for a user of a remote control vehicle security system to encode a receiver from a transmitter without any prerequisite skill or the need to even open the case of either the transmitter or the receiver.

It is an additional object of the present invention to provide a remote control vehicle security system where different types of transmitters may be provided and where each transmitter may operate with different numbers of possible code bits.

It is yet another object of the present invention to provide a remote control vehicle security system where several transmitters, each with a different code, may be added to or deleted from the system at will by the user.

It is another salient object of the present invention to provide a remote control vehicle security system which can be activated by one or more of a multi-billion number of possible codes, thereby providing code security of at least two thousand times the code security of prior art systems and yet which can be manufactured at a relatively low cost.

SUMMARY OF THE INVENTION

A remote control vehicle security system which is comprised of at least one receiver connected to electronic or electrical equipment which will enable or perform various functions when activated and one or more transmitters which can actuate the receiver by generation of a code or encoded signal. The receiver is operable with a control unit and this control unit is preferably a microprocessor controlled unit in accordance with the present invention. Moreover, the receiver and microprocessor control unit can perform all of the necessary decoding functions.

In one embodiment of the invention, one or more transmitters forming part of the system may have the provision of an encoder function included therein to generate encoded signals upon actuation of the transmitters. In a preferred form, the transmitter is a microprocessor controlled device for transmitting a plurality of different channel codes, and includes means for selecting a desired channel code and means for transmitting the selected channel code. This embodiment of the invention also comprises a receiver-control unit within the vehicle, and is responsive to the encoded signal to arm or disarm the system.

The control unit performs several primary functions including a decoding function. Thus, when the receiver receives the encoded signal, the microprocessor validates and decodes the transmitted signal. Thus, there is no requirement for the provision of a separate decoder.

The remote control vehicle security system of the present invention is also highly effective in that it is electronically user programmable. Moreover, no tooling or skills are required on the part of the user in order to program the receiver. The user is not even required to open the transmitter case or receiver housing when programming the system. The user of the system may initiate the receiver's program mode so that it will enable recording of subsequent messages or encoded signals received from the transmitter during the program mode. This may be accomplished by activating a program switch either mechanically, electronically or through voice recognition. Thereafter, the user actuates the transmitter, as for example, by pressing a switch on the transmitter. This will cause the encoded signal to be transmitted by the transmitter to the receiver.

The receiver and control unit will operate to decode the transmitted signal, and the decoded signal is then programmed into a memory unit, as hereinafter described, and becomes a "signature code signal" or "signature code word." In this sense, the system of the present invention is user programmable. Moreover, it is not necessary for anyone to know the specific signature code word programmed in the control unit, initially, or at any time thereafter. The control unit will, in effect, have received the signature code of the transmitter and will record that signature code in the control unit memory.

The receiver-control unit may be arranged so as to automatically exit the signature signal program mode after recording thereof. This automatic exit may occur, for example, after a certain time delay in which no further signal has been received. Otherwise, the receiver may be arranged so that it is manually switched by the user out of the program mode.

In a multi-channel form of the invention, the user selects a particular channel in which to record a signature code word, and once the selection is made, a received code word is recorded and assigned by the control unit to that selected channel. A plurality of signature code words may be stored for each channel. During the operating receive mode, received codes are compared to the stored codes for each channel, and when a match is formed, the control unit determines the channel to which the matched code corresponds and initiates a responsive action for that channel.

The receiver-control unit in the system of the present invention may also be operated by several transmitters, and each of which may be used to operate the receiver-control unit. Each transmitter may operate with a completely different code or encoded signal than any of the other transmitters, and in this case, the receiver will be responsive to each transmitter which has its code or encoded signal recorded in the control unit as a signature code word. It is not even necessary for the transmitters to be of the same type.

Each transmitter may have a different maximum number of digital code combinations. For example, one transmitter may have a ten-lit code and therefore is able to produce one thousand twenty-four possible combinations of unique codes. Yet another transmitter may operate with a thirty-two bit code, thus possessing more than four billion possible digital codes. The construction and the operation of these transmitters may be different and each may have a different number of switches and/or codes. However, each transmitter operates on the same frequency as the receiver.

If a plurality of individuals are required to have access to the arming and disarming of the system, each may be provided with the same or different transmitters. Each such individual will initially operate his or her transmitter to record the signature of that transmitter in the control unit memory, as one of the signature code signals. After this has been accomplished, each party using any one of the transmitters, whose signatures have been recorded, may then access the system by either arming or disarming the system, or enabling specific functions assigned only to one or more specific transmitters. Moreover, the system may be armed by one transmitter and disarmed by a second transmitter, re-armed by a third transmitter, and disarmed by a fourth transmitter, etc.

Any one of the transmitters may also be programmed out of the system, that is deleted from the system, by first entering the recording or program mode, and then programming repeatedly, the rest of the transmitters until the memory of the control unit is fully loaded.

In the event that any particular transmitter is lost or stolen, it is only necessary to erase the recorded signature code signals in the memory and re-record the signature code signals from the other transmitters which have not been lost or stolen. In this way, anyone who attempts to use the lost or stolen transmitter will not be able to arm or disarm the remote control access system. There is essentially no breach in security inasmuch as one must have access to the receiver-control unit which is located in the vehicle.

The microprocessor operated control unit also performs a reading function and a comparison function. In the reading operation, the control unit will read two or more successive and sequentially transmitted and decoded signals and will recognize them as correctly (authorized—not necessarily valid) transmitted signals, if two or more successive transmitted signals correspond. In this way, the control unit can determine if there is an error in transmission.

In the comparison function, the control unit will read a transmitted and decoded signal which is often referred to as a "received signal," and then compare that transmitted and decoded signal to each stored signature code or stored encoded signal which has been previously stored in the random access memory of the processor. Thus, and in this respect, the microprocessor operated control unit will perform a comparison function.

In the comparison operation, if the encoded signal which has been received and decoded does not correspond to a previously recorded signature code signal, the microprocessor will recognize that received and decoded signal as an invalid and unauthorized signal and will not enable a disarming or arming of the security system.

If the signal which has been decoded and compared does correspond to a previously recorded signature code signal and is thereby a valid signal, then the microprocessor will either enable or disable the system or initiate various commands. For example, if the security system was armed when the valid decoded signal was received for a predetermined channel, then the control unit will enable a disarming of the system. If the system was disarmed when the valid decoded signal is received, then the control unit will enable an arming of the security system.

The term "signal," and particularly with reference to an encoded transmitted signal or a received and decoded signal, is used in a general sense to refer to a transmitted or received code which may be comprised of a plurality of bits and/or bytes of information. Thus, as a simple example, in one of the embodiments of the system of the present invention, the encoded signal may be comprised of eighteen bits of information.

In view of the above, it can be observed that among the very significant advantages offered by the remote control security system of the present invention are the following:

1) The security system is self-programmable by a user in such manner as the user can merely actuate a switch-type element on the receiver and press a button on the transmitter for programming a selected code into the receiver as a signature code signal.
2) A signature code signal may be eliminated from the receiver-control unit by recording the codes of the desired transmitters several times until the memory of the control unit is fully loaded.
3) It is not necessary for anyone to know the code for triggering of the remote control system inasmuch as any code already programmed in the remote control transmitter will be automatically recorded into the control unit memory when the system is in the program mode and the remotely located transmitter is activated.
4) The security level of the present invention can be upgraded by the user at any time, as for example, by utilizing upgraded transmitters with a substantially greater number of digital codes, or the like. In this way, for example, the remote control system can be upgraded by the owner, at will, from 16,000 possible combinations of digital codes to over 4 billion possible digital code combinations without modifying or installing a new system.
5) In reading the encoded signal transmitted from the transmitter, a reading operation is conducted by the control unit associated with the receiver or two consecutive received signals to ensure that there is no error in the received signals before determining if that received and decoded signal compares to the signature control signal.
6) The transmitter and receiver are uniquely designed so that neither has to be opened and electronic or mechanical knowledge is not required for installing a new encoded signal at any time.
7) The remote control vehicle security system of the invention can operate with numerous types of transmitters, so long as they essentially operate at the same frequency range. This enables the purchase of transmitters from a source different from the receiver and control unit.
8) The remote control vehicle security system of the invention also uses significantly fewer electronic components than the prior art systems, and as an example, a decoder is not required inasmuch as the microprocessor can perform the decoding function.
9) A multi-channel system may be provided, wherein the control unit is operable during the programming mode to record a received code word and assign that stored word to a selected channel. Each of the channels may be electronically programmed and reprogrammed by the user.

This invention possesses many other advantages and has other purposes which may be made more clearly apparent from a consideration cf exemplary embodiments shown in the drawings accompanying and forming part of the present specification. They will now be described in detail for purposes of illustrating the general principles of the invention, but it is to be understood that such detailed description is not to be taken in a limiting sense.

BRIEF DESCRIPTION OF THE DRAWINGS

FIGS. 1A and 1B are respective block diagrams illustrating the major components of a remote control vehicle security system embodying the present invention.

FIG. 2 is a block diagram of a multi-channel form of the remote control, vehicle security system embodying the present invention.

FIG. 3 is a schematic electronic circuit view showing a portion of a transmitter which may be employed in a remote control vehicle security system of the present invention embodying the present invention.

FIG. 4 is a schematic electronic circuit showing one embodiment of a receiver forming part of a remote control vehicle security system embodying the present invention.

FIG. 5 is a schematic electronic circuit showing the control unit forming part of a remote control security system embodying the present invention.

FIG. 6 is a timing diagram of a plurality of wave forms showing a transmitted encoded signal.

FIGS. 7–16F illustrate simplified flow illustrative of the operation of a remote control vehicle security system embodying the present invention.

DETAILED DESCRIPTION OF THE DISCLOSURE

Referring now in more detail and by reference characters to the drawings which illustrate practical embodiments of the present invention, A (FIG. 1A) designates a remote control vehicle security system which comprises a transmitter unit **10**, a receiver **12**, and a microprocessor based control unit **14** with a control unit memory **14A**. The transmitter **10** is schematically shown as including an encoder **16** forming a part thereof. Moreover, the control unit 14 is shown with various functions which may be performed therein or in conjunction therewith. As an example, these functions may be performed by programming various steps into the control unit microprocessor, or otherwise, they could be performed by discrete apparatus carrying out the functions as identified. The control unit memory 14A may take the form of read only memory (ROM) buffers internal to a battery-backed microprocessor comprising the control unit 14, or a separate nonvolatile memory device such as an EEPROM communicating with the microprocessor to allow data to be read from or written into the memory by the microprocessor.

The preferred form of the transmitter unit 10 is a microprocessor-control unit as described in pending application Ser. No. 07/243,080, filed Sep. 9, 1988, entitled "Multi-Channel Remote Control Transmitter," by Ze'ev Drori and Moti Segal, and assigned to the same assignee of the present application. This pending application describes a multi-channel remote transmitter which permits convenient selection and transmission of a desired channel code. The transmitter operation is controlled by a microprocessor, which interfaces with a nonvolatile electrically erasable programmable read only memory (EEPROM) in which data including signature code data is stored. This pending application is incorporated herein by this reference in its entirety.

FIG. 1B illustrates additional elements of the vehicle security system, including the triggers and sensor devices 13 which are well known in the art, and the program and valet switches 11. The respective program and valet switches 11 are typically mounted within the vehicle at a location readily accessible to the system user. The devices 11 and 13 provide data input signals to the control unit 14. The control unit 14 includes outputs used to control various controlled devices in dependence on the system status and the input data, exemplary ones of the controlled devices being shown in FIG. 1A. The receiver 12 and control unit 14 will typically be installed within the vehicle at a location hidden from view, and perhaps even unknown to the vehicle owner. The transmitter 10 is shown in the form more fully described in pending application Ser. No. 07/243,080. This preferred form of the transmitter 10 is controlled by a microprocessor employing an EEPROM memory, and comprises a channel select switch actuated by the user to select a desired channel, and a transmit switch actuated to transmit the selected channel code.

FIG. 3 illustrates another embodiment of a transmitter unit which may be constructed in accordance with the present invention. The transmitter 10 generally comprises the encoder 16 which may be suitably encoded by the manufacturer so that the user is not required to encode the same. For this purpose, small switches may be provided on the encoder, or other means known in the art could be provided on the encoder for specifically generating an encoded signal. A plurality of output lines 18 extend from the encoder 16 in the manner as illustrated in FIG. 3. One such output line 18 is connected to the base of an NPN transistor 20 forming part of an oscillator transmitter 22. The conductor 18 is also connected through a resonator 23 which is, in turn, grounded. A resistor 24 is located in the conductor 18 and serves as a current limiter due to the fact that the transistor 20 is a low impedance device.

A capacitor 26 is connected across an additional pair of conductors 28 and 30, in the manner as shown, and which operates as a reset circuit. This ensures that the encoder will start the generation of each new encoded signal when actuated on each occasion.

In addition, a resistive-capacitive network 32 is also connected to the output of the encoder 16 in the manner as shown in FIG. 3, and comprises a pair of resistors 34 and 36 and a capacitor 38. This circuit arrangement stabilizes the length of each of the bits which are generated by the encoder 16. This is important in connection with the present invention in that the receiver and the control unit may measure the duration of the bit pulses in order to determine the status of these bits, that is, whether each is a "1" or a "0" bit.

The transistor 20 has a capacitor 40 connected across its emitter and collector in the manner as shown, and an additional capacitor 42 is connected to a resistor 44 on the emitter of &:he transistor 20. The capacitors 40 and 42 are generally provided for load matching purposes and the resistor 44 provides a control bias to the transistor 20.

Connected to the collector of the transistor 20 is a load circuit 46, as for example, a portion of an antenna load. This load circuit 46 is connected through a resistor 48 to the output conductor 28 of the encoder in the manner shown. A capacitor 50 is also connected to the load circuit 46 and is grounded. In effect, the point where the capacitor is connected to the load circuit, represents a ground level value. The resistor 48 and the capacitor 50 operate to decouple a battery as hereinafter described.

Also connected to the conductor 28 and to an additional conductor 52 are a pair of manually operable switches 54 and 56. These switches 54 and 56 are operable for providing two channels to the encoder. Thus, switch 54, when actuated, will cause the generation of a first encoded signal. Switch 56, when actuated, will cause the generation of a second encoded signal. A diode 58 is connected across the switches 54 and 56, and a diode 60 is also connected between the switches 54 and 56 and a battery 62.

The transmitter unit illustrated in FIG. 3 is a two-channel transmitter. In this way, two individual encoded signals could be generated by actuation of each of the switches 54 and 56 as aforesaid. The transmitter described in the referenced pending application, Ser. No. 07/243,080, is a multi-channel transmitter for generating many coded signals. However, it should also be understood that a single channel encoder could be used. Moreover, various multiple channel encoders, such as, for example, a three-channel encoder or a four-channel encoder, etc., could be employed with slight modification of the circuitry as described herein.

When any one of the switches 54 and 56 are closed, they will complete a circuit to the encoder 16, causing generation of an electrical signal over the conductor 18 and which is, in turn, transmitted as an encoded radio frequency signal, via the load 46 to the receiver 12.

The receiver 65 is more fully illustrated in FIG. 4 and generally comprises an antenna 70 for receiving the transmitted signals, which are coupled by capacitor 74 to an NPN transistor 72 which matches the impedance of the antenna 70, and operates as a radio frequency preamplifier. A resistor-capacitor network 76 is connected to the emitter of the transistor 72. A second resistor-capacitor network 78 is connected to the base of the transistor 72.

The collector of the transistor 72 is coupled via the conductor 80 to coupling capacitors 82 and 84. An

8-volt power source from the power supplies is connected to the collector of the transistor 72 through a resistor 84 which isolates the transistor 72 from the power supply and from the load.

Tank circuit 88 comprises a variable inductive device 90 for adjusting the receiver regenerative frequency. A capacitor 92 couples one end of the inductive device 90 to the conductor 80. The same end of the inductive device 90 is also coupled through capacitor 94 to a variable resistor 96, also connected to the 8-volt power source.

The conductor 80 is also connected to a local oscillator 98 which includes a transistor 100 having a capacitor 102 connected across its collector and, the conductor 80 being connected to the collector of transistor 100. The base of the transistor 100 is connected to the voltage source through the resistor 96. The emitter of the transistor 100 is connected to inductor 104. This arrangement of the local oscillator including the transistor 100, the capacitor 102 and the inductor 104 is designed to detect the pulses included in the received signal.

The inductor 104 is connected to conductor 106 which carries the detected signal. The detected signal pulses are passed through a resistor 108 and a capacitor 110 and to a signal amplifier 112 in the form of an NPN transistor. Another resistor 114 is connected across the collector and the base of the transistor 112, whose emitter is grounded and is also connected to a coupling capacitor 116.

The collector of the transistor 100 is connected to a pair of load resistors 118 and 120. The 8-volt power supply is connected through a load resistor 122 to the collector of the transistor 112. The reference voltage applied to the comparator 124 is developed by the voltage divider circuit comprising resistors 126 and 127. The comparator 124 receives a signal for comparison from the collector of the transistor 112 through a coupling capacitors 128 and 130. When the inputs to the comparator 124 compare, an output is generated and inverted by an inverter 132.

The output of the inverter 132 is then introduced into the control unit 14, as is more fully illustrated in FIG. 5. In this case, the output from the receiver 12 is introduced into an exclusive OR gate 140 (acting as a programmable inverter) which has an output to a microprocessor 142 with some internal RAM memory capacity, such as the NEC 80C49H microprocessor.

The microprocessor 142 receives a conductor carrying a reset input signal 144 from a reset signal generating circuit 145, as shown in FIG. 5. This reset signal generating circuit 145, which is sometimes referred to as a "watchdog" circuit, will automatically generate a reset signal each time that power is applied to the system, that is, each time that the system is "powered-up."

The reset signal generating circuit 145 may adopt any form of circuit which is capable of generating a reset signal. However, in the embodiment employed, a retriggerable one-shot is connected to and operable in conjunction with a standard one-shot and capacitor. The capacitor may be connected to the standard one-shot through an NPN transistor and grounded. The collector of the NPN transistor would then be connected to the conductor 144. This arrangement has not been illustrated or described in any further detail herein inasmuch as any standard resetting circuit arrangement could be employed.

The microprocessor 142 also receives a plurality of input signals 146A–N, 147 and 148. The input signal 147

represents a valet switch state, and the input signal 148 represents a program switch state, both from the valet and program switches which are typically located in the vehicle. The other inputs 146A–N into the microprocessor 142 are from the sensors and trigger devices 13 comprising the vehicle security system, for example, a hood lock trigger, a door trigger, a vibration sensor, etc. Otherwise, other forms of input signals may be generated and introduced into the microprocessor 142 in the same manner as any of the signals 146A–N.

The microprocessor 142 may be powered through the power supplies connected to the vehicle battery, and backed up by means of a battery circuit 150, as shown in FIG. 5 and which comprises a conductor 152. The conductor 152 may be connected to the 5-volt power supply in the manner as shown. Also located in the conductor is an NPN transistor 154 which effectively functions as a diode to prevent current from moving back toward the 5-volt source and only enables current to be delivered to the microprocessor 142. The gate of the NPN transistor 154 is connected to the collector of another NPN transistor 156. The base of this transistor 156 is connected between a voltage dividing circuit 158 which controls the threshold voltage applied to the microprocessor 142. A battery 160 and a diode 164 are connected in the manner as illustrated to provide back-up power in the event the vehicle battery is disconnected or disabled, thereby preventing loss of stored data in the RAM memory buffer. A grounding capacitor 166 is also connected to the conductor 152 in the manner as illustrated in FIG. 5.

As an alternative to the battery-backed microprocessor arrangement, an EEPROM memory device may be interfaced to the microprocessor 142 to provide nonvolatile memory buffers for storing the programmed data. The interfacing of a microprocessor to a peripheral device such as an external EEPROM is well known in the art. With this nonvolatile memory, the programmed data will be saved even in the event of power loss to the microprocessor.

The microprocessor 142 has a plurality of output signals 168A–N which are generally 4-volt signals and which are introduced into a buffer-amplifier 170. This buffer-amplifier 170 produces a plurality of outputs 172A–N. Moreover, each of the outputs 172A–N are connected to a 12-volt power source through coupling resistors 174 in the manner as illustrated, such that the outputs are raised to 12 volts. Each of the amplified signals 172A–N are then introduced into output circuits 176A–N in the manner as illustrated in FIG. 5.

The output circuits of FIG. 5 each generally comprise a field-effect transistor 178 which is connected through diodes 180 to a 12-volt power source. The various outputs from the output circuits 176 may provide responsive functions in the protected environment. For example, a first output 176A may actuate a siren. A second output 176B may provide for a pulsed alarm. A third output 176C may provide for an automatic door lock or an automatic unlocking of a door. Another output 176N may provide for an ignition cut-off, that is, so that the ignition of a vehicle could not be started in the event of an intrusion or an unauthorized entry into the vehicle. Other forms of outputs could similarly be provided.

A special output from the microprocessor 142 in the form of a hood unlock signal is introduced into an inverter assembly 182 and then into an NPN transistor 184 which amplifies the signal. A coupling resistor 186 connects the base of the transistor 184 to the output of the inverter. The collector of the transistor 184 is connected to an output circuit 188 which is also comprised of a field effect transistor 190. This signal serves to automatically unlock the hood when generated. The generation of the hood unlock signal is authorizedly initiated by the control unit 14 of the system for a thirty-second time period after initially disarming the system.

Additional outputs from the microprocessor 142 are the decoder channel outputs CH 2 . . . CH N which are activated by receipt of a valid signature code word for the respective channels. Upon receipt of such a valid code word, the corresponding channel output will be activated for a minimum period of 0.5 seconds.

Also connected to the microprocessor 142 is an oscillator control circuit 192 comprised of a crystal oscillator 194 and having a pair of capacitors 196 connected to the outputs thereof. This crystal oscillator 192 generates a control frequency which controls the speed of operation of the microprocessor 142 and generates the clocking signals therefore.

The microprocessor 142 also generates a plurality of control light outputs 198 which may control light emitting diodes 200 or other forms of light emitting devices. A pair of these signal light outputs may inform the user whether the system is turned on or off, and a third of the signal light outputs may inform the user if the microprocessor is running code in a correct sequence. It should be understood that other forms of output signal lights for generating other informational outputs may be employed in accordance with the present invention.

Referring now to FIGS. 7-16, the operation of the system is shown in simplified flow diagram form. FIG. 7 is a flow diagram illustrating the primary routines of the main program loop implemented by the control unit microprocessor. Upon entering the main loop, the RESET routine 302 is called, to initialize the system parameters. This routine is entered when power is applied to the system controller microprocessor, and is described more fully with respect to FIG. 8.

The next routine called during the main loop operation is the CHECK RECEIVER routine 304. This routine monitors the receiver operation to determine when a complete word has been received, and to determine whether the received word corresponds to a stored signature code word. This routine is described more fully with respect to FIGS. 10A-10E.

The ALARM MODE routine 306 determines whether the alarm conditions are present, and activates the appropriate flags and signals to cause the alarm events to be activated, such as a siren. Such an alarm mode routine is described in the pending application, Ser. No. 07/231,159, filed Aug. 11, 1988, entitled "Electronic Vehicle Security System," by Ze'ev Drori and Amir Abrishami and assigned to the assignee of this application. The entire contents of this co-pending application are incorporated herein by this reference.

The VALET MODE routine 308 is called next, and its purpose is to configure the system so that the vehicle may be left with a service garage or parking attendant without causing activation of the alarm system inadvertently. Such functions are per se known in the art. The VALET MODE routine is described more fully with respect to FIG. 11.

The CHECK TRIGGERS/SENSORS routine 310 is called next. Its purpose is to check the status of the system sensors and triggers 13. The status is determined by the interrogation of the input signals 146A-N to the microprocessor 142.

The CONTROL routine 312 determines whether the system should be armed or disarmed, and will be described more fully with respect to FIG. 12. Depending on the armed/disarmed state of the system, either the DISARMED MODE routine 316 or the ARMED MODE routine 318 will be called. These routines perform the various monitoring and housekeeping functions required during the respective states of the system. Similar functions are described in the pending application Ser. No. 07/231,159.

The next routine to be called is the LED CONTROL routine 320, which controls the LEDs 200. The OUTPUTS CONTROL routine 322 serves to turn on and off the output signals from the microprocessor in order to control the various output devices associated with the system. Similar functions are also described more fully in the pending application Ser. No. 07/231,159.

The DECODERS OUTPUT CHANNELS CONTROL routine 324 controls the various channel output states in dependence on the decoded received signals. This routine is described more fully with respect to FIG. 13.

The final routine in the main loop is the ENTER PROG MODE. This routine is called to perform the various programming functions carried out, including the programming of the transmitter signature code signals. Two alternate routines are disclosed in FIG. 15 and FIGS. 16A-F, respectively. Operation then loops back to routine 340, and the loop is repeated again. The routine is repeated continuously so that, for example, the various sensors and triggers are interrogated and the receiver output is checked many times per second.

The RESET routine 302 is shown more fully in FIG. 8, and comprises the steps of initializing the input and output terminal conditions of the microprocessor (step 330) and initializing the random access memory registers (step 332) comprising the microprocessor 142 in which data is stored during the system operation. This routine is entered after the system has powered up, which will typically occur only if the vehicle battery has been disconnected and then reconnected, since the system receives power from the vehicle battery continuously even when the vehicle ignition is turned off. As a security feature described more fully in pending application Ser. No. 07/138,828, the alarm condition will be declared unless the ignition switch is turned on while the battery is reconnected. Thus, at step 334 the ignition switch is checked and if on, the ARM flag is cleared and the program operation returns to the main loop. If the ignition switch is not on, then at step 338 the ARM and TRIP flags are set and operation returns to the main loop. (Active ARM and TRIP flags will call activation of the alarm siren.)

A microprocessor operation which is conducted in the background of the main loop operation on an interrupt basis is the RECEIVER BIT ASSEMBLER routine illustrated in FIG. 9. The purpose of this background routine is to assemble on a real time basis the bits of a received signal as they are received. The bit format employed in this embodiment is illustrated in FIG. 10B, wherein the width of each pulse determines whether the pulse represents a "1" or a "0." A "1" pulse is longer than a "0" pulse as illustrated in FIG. 10B. A signature code signal or word comprises a predetermined number of bits, such as N bits, M bits or the like. Successive transmitted code signals or words are separated in time by "quiet" periods as shown in FIGS. 10C and 10D; FIG. 10C representing an N bit word format and FIG. 10D representing an M bit format where N does not equal M, M in this case being fewer bits than N.

Step 350 of the RECEIVER BIT ASSEMBLER routine of FIG. 9 determines whether the receiver output is on a falling edge, and if not, the time is registered (step 352) and operation branches to step 366 where the quiet period timer is reset.. If a falling edge is detected, then the bit time is calculated (step 354), and if the bit length corresponds to a "0," a "0" bit is shifted into the received word buffer of the microprocessor (step 358). Otherwise the bit is determined to be a "1," and a "1" bit is shifted into the buffer. If the bit counter for the word length equals N step 362), the predetermined length of the signature code word, the counter is reset (step 364), and the quiet period timer is reset (step 366). If the bit counter does not equal N, then step 364 is bypassed. Operation then returns to the main loop operation from wherever the interrupt occurred.

The CHECK RECEIVER routine is illustrated in further detail in FIG. 10A. At step 370, the quiet period timer is checked, and if it has not timed out, operation returns to the main loop. If the timer has timed out, indicating that the complete word has been received, then the bit counter is checked. In this embodiment, the possible signature code lengths are N and M bits. Thus, if the received word length is either N (step 372) or M (step 374), then the bit counter is reset (step 375) and the COMPARE subroutine 376 is called. If the word length does not equal either M or N, then the received word cannot be a valid signature code word and operation returns to the main loop.

The COMPARE subroutine is illustrated in FIG. 10E. If the received code is all zero bits (step 400), operation returns to step 378, since all zero words are considered illegal codes. The microprocessor maintains two code buffers, one for storing the previously received code word, the other for storing the present received code word. If the present received code word does not match the previously received code word (i.e., two identical code words have not been successively received) at step 402, the presently received code word is moved to the previous word buffer (step 404) and operation returns to the main loop. If the presently received code word matches the previous code word, then, if the system is in the transmitter program mode (step 406), the "PRGM VALID CODE" flag is set (step 408) and operation returns.

If the system is not in the transmitter programming mode, then at step 410 the address for the first stored signature code word to be compared is set, and the received code is compared with this stored code word (step 412). If the received code word is identical with the stored signature code word, then the VALID CODE flag is set, the code address pointer (indicating the channel number) for the matched stored signature code word is saved (step 414) and operation returns to step 378. If a match is not found, then if the code has not been compared against all stored signature code words (step 416), the address for the next stored word to be compared is set (step 420), and operation loops back to step 412 to perform the comparison. If the received code has been compared with all stored signature control words, then at step 418 the CODE VALID flag is reset or cleared, and operation returns to step 378.

At step 378, if the system is in the transmitter programming mode, operation returns to the main loop. If not in the transmitter programming mode, then if the CODE VALID flag is not set, operation returns to the main loop. If the flag is set (step 380), then if the received code was the channel 1 code word, the CH 1 ON flag is set, the CH 1 timer is reset to 0.5 seconds (step 384), and operation returns to the main loop. I the received code is the channel 2 code word (step 386), then the CH 2 ON flag is set, and the CH 2 output timer is set to 0.5 seconds. Operation then returns to the main loop.

The VALET MODE routine is illustrated in FIG. 11. Here, if the system is in the VALET MODE at step 430, i.e., if the VALET flag is already set, operation returns to the main loop. If not, then at step 432 the ignition switch is checked, and if not on, operation returns to the main loop. If the ignition switch is on and if the valet switch is on (step 438), then the VALET flag is set and operation returns to the main loop. If the valet switch is not on, the VALET flag is reset or cleared (step 436) and operation returns to the main loop. Thus, in order to enter the VALET MODE, both the ignition and valet switches must be on.

The CONTROL routine is shown in FIG. 12. In this embodiment, channel 1 is used to arm and disarm the system (for a single channel system embodying the invention, that channel is used to arm and disarm). If the CH 1 ON flag is set at step 450 indicating receipt of a valid signature code word for channel 1, then if the flag was not set since the last pass through this routine (step 452), the panic timer is checked at step 454. This timer measures the length of time the code has been transmitted repeatedly, and if the timer has not timed out (2.5 seconds), operation returns to the main loop. If the timer has expired, the PANIC flag is set (step 456) indicating that the transmitter user desired to trigger an alarm condition and operation returns. If the CH 1 ON flag has just been activated (step 452, then if the system is presently in the armed state (step 460), the DISARM routine is called (step 462) to disarm the system. If the system is presently in the disarmed state, then the ignition switch is checked at step 463, and if on, operation returns to the main loop. This is to prevent the system from being armed while the vehicle is being driven to prevent a safety hazard. If the ignition switch is not on, then the system considers it safe to arm the system, and the ARM routine is called for this purpose (step 464).

FIG. 13 illustrates the DECODER OUTPUT CHANNELS CONTROL routine. Step 470 checks the CH 1 on flag and if on, the timer for channel 1 is checked. This is a 0.5 second timer, and if it has timed out, then at step 476, the CH 2 ON flag is checked, and if it is set, then the channel 2 timer is checked (step 478). If it has timed out, then the CH 2 ON flag is reset. If the timer has not timed out, then operation returns to the main loop. Thus, once set, the channel on flags remain set for 0.5 seconds after the receipt of the valid code for that channel. Of course, if the system employs more than two channels, then the additional channel flags, e.g., CH3 ON, CH4 ON, and so on, will be checked and corresponding microprocessor output activated when a channel flag is active.

FIGS. 14–16 illustrate the system programming mode. FIG. 14 illustrates the ENTER PROG MODE routine. In this embodiment, the program mode is entered by turning on the ignition switch and actuating the program switch. Thus, at step 500 the ignition switch is checked, and if not on, and if the program mode had not been entered prior to this pass through the main loop (step 504), operation returns to the main loop. If the programming mode has been entered, then an acknowledgement chirp is sounded indicating exit from the program mode (step 506) and operation returns to the main loop. If the ignition switch is on, then the program switch timer is checked and if it has timed out, step 504 is carried out. The program switch timer measures how long the program switch has been actuated, the program mode being entered only when the program switch has been actuated for at least a predetermined time duration, say 1 second. The switch timer duration is set to the predetermined time duration, so that when the switch timer times out, the program mode is entered. If the timer has not timed out, then at step 508, if the program mode has already been entered, the subroutine PROGRAM MODE is immediately called (step 514). If the program mode had not previously been entered, the program switch is checked (step 510) and if it is not active, operation re&urns to the main loop since this indicates that the program mode has not been selected by the user. If the program switch is active, then the program switch timer is checked and if it has not timed out, operation returns to the main loop. If the program switch timer has timed out, the program timer is set to one minute (step 514) the subroutine PROGRAM MODE is now called (step 516). The program timer in this embodiment has a predetermined duration of one minute, and allows a one minute interval after the last user programming activity before automatically terminating the program mode.

FIG. 15 illustrates the PROGRAM MODE subroutine for a single channel system. Because there is only one channel to be recorded, no additional programming selection tasks are required. At step 518A, an acknowledgement chirp is sounded indicating to the user that the program mode has been entered. At step 518B, the signature code word memory buffer is checked to determine whether the buffer is full. In this embodiment, the buffer capacity is predetermined, for example, eight possible code word addresses. If the buffer is full, i.e., with all eight addresses containing data, then at step 518C, the address pointer is initialized to the first code address in the buffer, since the new code will be stored in this first code memory location, with the previous contents being erased. Otherwise, if the buffer if not full, the address is set to the first empty buffer code address (step 518D). At step 518E, the new code received by the system is stored in the code buffer. The new code is then compared with the other stored code words (518I) and if there is a match (i.e., the identical code is already stored in the buffer), and if this code is the one just stored, then it will be erased. This prevents the same code from being stored in the memory at more than one location. Operation then returns to the main loop.

FIGS. 16A-F illustrate the PROGRAM MODE for the case of a multi-channel system with multiple feature programmability. As shown in FIG. 16A, there can be provided various programming options for selection by the user. A mean for selecting one of the programming options is described in the pending application Ser. No. 07/231,159, wherein the user may select one of the options by manipulating the program and valet switches after entering the programming mode. FIG. 16B shows a selection procedure for selecting the REMOTE CONTROL programming option as well as other options, and is described more fully in the pending application Ser. No. 07/231,159.

Assume that the user has now selected the REMOTE CONTROL option, so that the routine shown in FIG. 16C has been called. An appropriate number of acknowledgement chirps is sounded (step 520) to indicate that the remote control programming option has been selected and entered. At step 522, the determination is made as to whether the user has selected for programming channel 1/channel 2, and if so, a corresponding chirp message is sounded (step 524) and the PROG CH 1/CH2 subroutine is called. If the system has channels 3 and 4, then the CH3/CH4 subroutine may be selected (steps 528, 530 and 532). There may even be provided an option for combined programming of the channels 3 and 4, and this option may be selected also (steps 534, 536 and 538).

FIG. 16D shows the PROG CH1/CH2 subroutine, which selects either the channel 1 or channel 2 for programming. At step 550, if there has not been received, a complete code word operation returns to FIG. 16B. If a complete word has been received, then if the valet switch is on, channel 2 programming has been selected and the PROGRAM CH 2 subroutine is called (steps 552 and 554). If the valet switch is not on, then the channel 1 programming has been selected and the PROGRAM CH1 subroutine is called.

FIG. 16E illustrates the PROGRAM CH1 subroutine, which is very similar to the single channel program mode shown in FIG. 15. In this case, however, the allowable code addresses in which a new code word may be stored are those reserved for the channel 1 signature code words in the code buffer, as indicated in the simplified memory buffer map of FIG. 16F, showing respective memory locations for the respective exemplary channels 1-4. In comparing the new stored code word against the buffer contents for duplicate stored code words, however, all channel locations are searched, so that the same code word is not stored in more than one channel buffer. The PROGRAM CH2 subroutine is similar to the PROGRAM CH 1 routine, except that the allowable code addresses in which the channel 2 signature codes may be stored are those reserved for the channel 2 signature code words.

A selection routine may be employed for selecting between the channel 3 and channel 4 programming option similar to that shown in FIG. 16D for channels 1 and 2. Similarly, the PROGRAM CH3 and PROGRAM CH 4 subroutines are similar to the PROGRAM CH 1 subroutine described above.

Thus, a multi-channel system may be employed in which a predetermined number of code words may be stored in the memory of the control unit for enabling or disabling the various channels of the system. In this embodiment, the channel 1 codes are used to arm or disarm the security system. The remaining channels may be employed to enable or disable a desired function, e.g., a trunk release, a hood release, a power window function or the like.

OPERATION OF THE SYSTEM

The operation of the security system has been described in connection with the detailed description thereof. However, the following should provide a brief summary of the operation of the various embodiments of the system.

The transmitter unit 10 may be operated by actuation of the channel select and transmit switches for the transmitter embodiment of FIG. 1B, or one of the switches 54 or 56 for the transmitter embodiment of FIG. 3. The transmitter will thereupon generate a coded signal which is transmitted as an encoded radio frequency signal. The encoded transmitted signal is then received by the receiver 12, which will process the signal and generate an electrical signal output at the inverter 132. The signal from the inverter 132 is introduced into and decoded in the control unit 14.

When the user desires to match a transmitter 10 to the receiver control unit 14, the system will first be placed in the program mode. This may be accomplished, in the case of a single channel system, by actuating the program switch into a program position. (The switch may be activated manually or electronically or through voice recognition.) In a multi-channel system the user enters the program mode and selects the particular channel to which the transmitted signal is to be recorded. When the system is then in the program mode, a transmitter which is to have its signature code signal recorded therein is actuated to generate an encoded signal. This encoded signal will then be recorded as a signature code signal in the memory of the control unit 14. If only one transmitter is actuated while the control unit 14 is in the program mode, only a single signature code signal will be recorded in the control unit 14. If additional transmitters are actuated when the control unit 14 is in the program mode, each of those actuated transmitters will have its own signature code signal recorded. The control unit 14 will exit the program mode automatically after a preset duration where the control unit 14 is then in a condition to decode subsequent received encoded signals.

In the case of the multi-channel system, the user selects the particular channel into which the transmitter code is to be recorded, and thereafter the transmitter is actuated with the resulting received code being storing automatically in the memory buffer corresponding to the selected channel.

All subsequent signals will be compared against the recorded signature code signals. If any subsequent signal is identical to any of the signature code signals, then it will be recognized as a valid encoded signal and will thereupon arm or disarm the security system, in the case of a single channel system. However, if the subsequent signal does not conform to the signature code signals which have been recorded, then the subsequently transmitted and decoded signals will not arm or disarm the security system. In the multi-channel system, the control unit determines the corresponding channel of a valid received code and takes appropriate action in dependence on that channel. Thus, a channel 1 code will arm or disarm the system, a channel 2 code will activate the channel 2 output, and so on.

The transmitter may be capable of generating one or more individual encoded signals or channel codes, e.g., by actuation of the switches 54 and 56 in the transmitter embodiment of FIG. 3. Thus, either of the encoded signals from a single transmitter may be used to operate the control unit 14.

The user of the system can also easily delete one of the transmitters from the system by removing the signature code signal of that transmitter from the control unit. In this case, the signature code signal of the transmitter can be deleted from the system, depending upon the specific programming of the control unit 14. In one of the preferred embodiments, if the control unit 14 is placed in the program mode and the signature code signal is generated on a plurality of successive occasions, the number being equal to the number of code word locations assigned to storage of the signature code words, such as eight successive occasions in close sequence, that will cause an automatic deletion of the signature control signal and hence, that transmitter from the system. This results from the above-described program mode operation, wherein pre-existing stored rode words are successively erased once the particular channel buffer is full.

In accordance with the above-identified circuit arrangement, it can be understood that it is not necessary for the user or the dealer or the installer of the system to either understand or to have knowledge of the specific encoded signal which is generated in order to add or delete any transmitter from the remote control access system. Thus, the user does not have to actuate any predetermined number of switches or other input means, such as scratch a circuit pattern on a printed circuit board in order to generate the encoded signal. Indeed, the user or dealer or installer does not have to possess and use any of the special techniques for encoding the transmitter and which usually require the intervention of skilled personnel. Moreover, it is not even necessary for the user or the dealer or installer to open either the transmitter or the receiver in order to record the signature control signal.

When the security system in the program mode and when a signal is transmitted from any one or more transmitters, that signal will be received by the receiver 12 and decoded by the control unit 14. After decoding, the received signal will then be recorded in the memory of the control unit as a signature code signal. This will occur with each signal received from any transmitter when in the program mode. When the security system is in the operating-receive mode, no further recording can be accomplished until the system is switched back to the program mode. When in the operating-receive mode, if any encoded signal are generated and received by the receiver, they will be decoded and compared against the recorded signature code signals which have been recorded in the memory unit. If there is no valid comparison with any signature code signal, the received signal will be recognized as an invalid signal and will not arm or disarm the system.

Additional transmitters can be quickly and conveniently added to or deleted from the security system without the intervention of skilled personnel, such as a dealer or installer. The remote control vehicle security system is also highly effective in that it may be used with many transmitters and also many different types of transmitters and with transmitters operating on different coded bases. The use of the system with a plurality of differing types of transmitters is more fully illustrated in FIG. 2 of the drawings.

In this case, it can be observed that a first transmitter 10A comprising encoder 16A generates a first code A1. This transmitter 10A will generate a second code A2 if a pair of channels are provided on this transmitter. For this purpose, the transmitter shown in FIG. 1A or the circuit arrangement of FIG. 3 would be employed utilizing both switches 54 and 56. In like manner, a second transmitter device 10B comprising an encoder 16B is provided for purposes of generating a code B1 and an encoded signal B2. Finally, a third transmitter 10C comprising an encoder 16C is capable of generating a first encoded signal C1 and a second encoded signal C2. As also indicated previously, any of these transmitters could be used with more or less than two channel codes for generating any desired number of channel codes.

In accordance with the arrangement as illustrated in FIG. 2, it can be observed that each of these transmitters and encoders may be of different types and each will generate different encoding signals. Nevertheless, on the first occasion when each of these transmitters are used, they will be used in such manner so as to operate the control unit 14 to record a signature code signal. Thus, each of the three transmitters 10A, 10B and 10C will have their signature code signal recorded in the control unit. On each subsequent occasion, when they are actuated, they will be capable of arming and disarming the security system in the manner as previously described.

One of the unique aspects of this invention is the fact that any conventional transmitter can be used as long as it is operating on the same frequency as the receiver 12 and employs the same bit code format, such as pulse width modulation. Thus, if the user of the system loses one of the transmitters or desires to upgrade the system with another transmitter with more digital codes and higher security, it is not necessary to install an entirely new system. The user merely buys another transmitter and records the signature code signal in the microprocessor of the control unit 14.

Moreover, it is important to note that each transmitter is not required to generate the same encoded signal. Thus, the user may merely provide additional authorized parties wi&:h transmitters for obtaining access to the security system without an elaborate time consuming and costly recording of a particular transmitter. It is necessary to only record once the signature code signal of that transmitter in the control unit, as aforesaid

In accordance with the present invention, it is also possible to simultaneously use any number of coded combinations, as for example, an M-bit, e.g., where M=14, encoded signal which could result in sixteen thousand encoded signal combinations. In like manner, it is possible to use an N-bit, e.g. where N=20, signal which could result in up to one million encoded signal combinations, etc. In essence, the system of the present invention is virtually unlimited to the number of codes which can be used or the number of bits in any encoded signal. The code memory reserves memory locations for a predetermined number of code words for each channel, e.g., eight possible signature code words for channel 1, but the bit length of each word is not preassigned. Thus, the signature code words may comprise different numbers of bits.

The system of the invention is also capable of comparing two or more sequential encoded, transmitted and decoded signals to ensure that they are identical to one another. Thereafter, if the subsequently decoded signals are identical, they are then compared to the signature code signals. If the decoded signals match the signature code signal, then it is deemed to be a valid transmitted signal for purposes cf arming or disarming the security system be a valid transmitted signal for purposes of arming or disarming the security system.

This arrangement for signal matching is more fully illustrated in FIG. 6 of the drawings. It can be observed that a signature code signal is shown in the upper portion of FIG. 6. The first of the bits, designated as 202 is a wider bit than another one of the bits 204 and, thus, the bit 202 may represent, for example, a "1" signal, whereas the bit 204 may represent a "0" signal. Located beneath the signature signal is the transmitted signal which may have been decoded in the control unit. In this case, it can be observed that the transmitted signal is identical to the signature signal.

The transmitted signal has length of n bit[, in the manner as illustrated in FIG. 6. Located to the right of the transmitted signal is a second transmitted signal. In this case, it can be observed that the second transmitted signal is shown to be duplicate of the first transmitted signal. In this way, the two transmitted and decoded signals will compare in the comparator of the control unit. As a result, they will form a signal combination which may be compared against the signature code signal. In this case, it can be observed that the two transmitted signals are identical and are also identical to the signature code signal. As a result, the microprocessor operated control unit will recognize this as a valid decoded signal, enabling the user to have access to the security system for purposes of arming or disarming the same.

If the second transmitted and decoded signal is not identical to the first transmitted signal, then there is no further comparison with respect to the signature control signal. There must be at least two or more sequential transmitted and decoded signals which are identical to one another before an comparison to the signature code signal can take place and hence, there must be the same comparison before any arming or disarming of the system can occur.

The microprocessor may also measure various other characteristics of the bits in order to determine whether or not a decoded signal is a valid signal. For example, the microprocessor could examine and compare bit length, the number of bits and widths of the bits. Other characteristics, for example, amplitude or the like could also be used for determining whether a decoded signal is a proper or valid decoded signal.

It is understood that the above-described embodiments are merely illustrative of the possible specific embodiments which may incorporate principles of the present invention. Other arrangements may readily be devised in accordance with these principles by those skilled in the art without departing from the scope of the invention.

What is claimed is:

1. An electronically programmable remote control vehicle security system, comprising:

a precoded portable hand-held transmitter comprising means for generating and transmitting a predetermined fixed, digitally encoded, radio frequency, receiver-responsive signal representative of a predetermined fixed transmitter code, and actuating means for actuating said generating and transmitting means so that said signal is automatically generated and transmitted upon actuation;

vehicle antitheft means;

a system control unit disposed within said vehicle, comprising:

(i) receiving means operable during a system program mode and a system operating-receiving mode for receiving said transmitted encoded signal and generating an electrical signal representative of the encoded signal;

(ii) a digital memory for storing data representative of signature code signals;

(iii) programming means for recording in said digital memory received signals for arming or disarming said vehicle antitheft means, said means activated only during said system program mode for automatically storing in said memory received signals representative of said predetermined transmitter code as a signature control signal for arming or disarming said vehicle antitheft means; further characterized in that said program mode is automatically terminated after a predetermined time delay from receipt of the last transmitted encoded signal during said program mode;

(iv) operating means activated during said operating-receiving mode for comparing received electrical signals with said signature control signal stored in said memory means to determine if said electrical signals correspond to said recorded signature code signal, and means for arming or disarming said vehicle antitheft means in response to received signals corresponding to said signature code signal stored in said memory; further characterized in that said system control unit comprises a user-accessible switch disposed in said vehicle, and said access control unit is responsive to the position of said switch for entering said program mode; and

wherein said transmitter and said receiving means cooperate to form a one-way radio frequency signal transmission link for communicating signals only from said transmitter to said receiving means, said transmission link being employed by said system during said programming mode for transmitting said encoded signals from said transmitter to said access control unit to be stored in said memory as said code signals, said link further employed during said operating receiving mode for transmitting said encoded signals from said transmitter to said control unit.

2. An electronically programmable remote control vehicle security system, comprising:

a precoded portable hand-held transmitter comprising means for generating and transmitting a predetermined fixed, digitally encoded, radio frequency, receiver-responsive signal representative of a predetermined fixed transmitter code, and actuating means for actuating said generating and transmitting means so that said signal is automatically generated and transmitted upon actuation; wherein said transmitter is suitably encoded with said predetermined transmitter code by the manufacturer thereof so that the system user is not required to encode said transmitter;

vehicle antitheft means;

a system control unit disposed within said vehicle, comprising:

(i) receiving means operable during a system program mode and a system operating-receiving mode for receiving said transmitted encoded signal and generating an electrical signal representative of the encoded signal;

(ii) a digital memory for storing data representative of signature code signals;

(iii) programming means for recording in said digital memory received signals for arming or disarming said vehicle antitheft means, said means activated only during said system program mode for automatically storing in said memory received signals representative of said predetermined transmitter code as a signature control signal for arming or disarming said vehicle antitheft means;

(iv) operating means activated during said operating-receiving mode for comparing received electrical signals with said signature control signal stored in said memory means to determine if said electrical signals correspond to said recorded signature code signal, and means for arming or disarming said vehicle antitheft means in response to received signals corresponding to said signature code signal stored in said memory; and

wherein said transmitter and said receiving means cooperate to form a one-way radio frequency signal transmission link for communicating signals only from said transmitter to said receiving means, said transmission link being employed by said system during said programming mode for transmitting said encoded signals from said transmitter to said access control unit to be stored in said memory as said code signals, said link further employed during said operating receiving mode for transmitting said encoded signals from said transmitter to said control unit.

3. An electronically programmable remote control vehicle security system, in which a receiver and a control unit therefor are operable upon receipt of a proper transmitted encoded signal from any of a plurality of transmitters to arm or disarm said vehicle security system, said system comprising:

at least one first transmitter capable of transmitting a first receiver responsive, radio frequency, digitally encoded signal comprising an N-bit digital code word for arming and disarming said system, said transmitter comprising actuating means for actuating said transmitting of said signal so that said first signal is automatically transmitted upon actuation;

at least one second transmitter capable of generating and transmitting a second receiver responsive, radio frequency, digitally encoded signal comprising an M-bit digital code word for arming and disarming said system, said second transmitter comprising actuating means for actuating said transmitting of said second signal so that said second signal is automatically transmitted upon actuation;

wherein N and M are each integer values and N need not equal M;

vehicle antitheft means;

a receiver located in said vehicle and responsive to the transmitted radio frequency encoded signals during a system programming mode and a system operating-receiving mode for generating electrical signals corresponding to each of the respectively encoded signals;

said receiver and said first and second transmitters comprising at least first and second one-way radio frequency signal transmission links for communicating signals only from said first or second transmitters to said receiver during said system programming and system operating-receiving modes; and

a control unit operatively associated with the receiver, said control unit comprising:

(i) means for decoding said electrical signals to generate respective decoded digital signals representative of said N-bit code word and said M-bit code word;

(ii) a digital memory for storing said N and M-bit code words;

(iii) means operable in said system program mode for automatically recording in said digital memory said respective decoded digital signals received and decoded during said program mode as first and second signature code signals representative of said N-bit code word and said M-bit code word;

(iv) means activated during an operating-receiving mode for comparing received and decoded signals to said first and second signature code signals which have been previously recorded during said program mode to determine if said decoded digital signals correspond to either of the recorded signature code signals and thereby represent valid signals for arming or disarming said vehicle antitheft means; further

characterized in that the system is user programmable such that the user of any transmitter may initially record the encoded signal from that transmitter as a signature code signal in the control unit by simple actuation of the transmitter when the system is in said program mode for recording signature control signals for arming or disarming said vehicle antitheft means, thereafter only requiring the transmission of the encoded signal from the transmitter for recording as a valid signature code signal, and whereby said signature control signal is automatically recorded in said digital memory; further

characterized in that said system is provided with a switch disposed in said vehicle to put the receiver in the program mode for recording said arming/disarming signature control words; and further characterized in that said system program mode is automatically terminated after a pre-established time delay from receipt of the last transmitted encoded signal during said program mode.

4. An electronically programmable remote control vehicle security system, in which a receiver and a control unit therefore are operable upon receipt of a proper transmitted encoded signal from any of a plurality of transmitters to arm or disarm said vehicle security system, said system comprising:

at least one first transmitter capable of transmitting a first receiver responsive, radio frequency, digitally encoded signal comprising an N-bit digital code word for arming and disarming said system, said transmitter comprising actuating means for actuating said transmitting of said signal so that said first signal is automatically transmitted upon actuation;

at least one second transmitter capable of generating and transmitting a second receiver responsive, radio frequency, digitally encoded signal comprising an M-bit digital code word for arming and disarming said system, said second transmitter comprising actuating means for actuating said transmitting of said second signals so that said first signal is automatically transmitted upon actuation;

wherein N and M are each integer values and N need not equal M;

vehicle antitheft means;

a receiver located in said vehicle and responsive to the transmitted radio frequency encoded signals during a system programming mode and a system operating-receiving mode for generating electrical signals corresponding to each of the respectively encoded signals;

said receiver and said first and second transmitters comprising at least first and second one-way radio

frequency signal transmission links for communicating signals only from said first or second transmitters to said receiver during said system programming and system operating-receiving modes; and

a control unit operatively associated with the receiver, said control unit comprising:

(i) means for decoding said electrical signals to generate respective decoded digital signals representative of said N-bit code word and said M-bit code word;

(ii) a digital memory for storing said N and M-bit code words;

(iii) means operable in said system program mode for automatically recording in said digital memory said respective decoded digital signals received and decoded during said program mode as first and second signature code signals representative of said N-bit code word and said M-bit code word;

(iv) means activated during an operating-receiving mode for comparing received and decoded signals to said first and second signature code signals which have been previously recorded during said program mode to determine if said decoded digital signals correspond to either of the recorded signature code signals and thereby represent valid signals for arming or disarming said vehicle antitheft means; and wherein said first and second transmitters are respectively suitably encoded with said N-bit and said M-bit digital codes by the respective manufacturer thereof so that the system user is not required to encode said respective transmitters.

5. A vehicle security system in which a control unit is responsive to receipt of a proper transmitted encoded radio frequency signal from a transmitter to arm or disarm said system, comprising:

vehicle antitheft means, said means comprising a vehicle ignition disabling means;

a portable hand-held transmitter comprising means for generating and transmitting a predetermined fixed digitally encoded, radio frequency, receiver-responsive signal representative of a predetermined transmitter code; and

a control unit located within said vehicle, comprising:

(i) radio frequency signal receiving means operable during said program mode and during said system operating-receiving mode for receiving said transmitted encoded signal and generating an electrical signal representative of the encoded signal;

(ii) a digital memory for storing signature code signals;

(iii) programming means for recording in said digital memory received signals for arming or disarming said vehicle antitheft means, said means activated only during a system program mode for automatically storing in said memory said electrical signals representative of said radio frequency, receiver-responsive received signals representative of said predetermined transmitter code as a signature code signal for arming or disarming said vehicle antitheft means; and

(iv) operating means activated during an operating-receiving mode for comparing received electrical signals with said signature code signal stored in said memory means to determine if said electrical signals correspond to said recorded signature code signal and for arming or disarming said antitheft means if said electrical signals correspond to said recorded signature code signal, wherein said transmitter and said receiver means cooperate to form a one-way radio frequency signal transmission link for communicating signals only from said transmitter to said receiving means, said transmission link being employed by said system during said programming mode for transmitting said signal representative of said transmitter code to said access control unit to be stored in said memory means as signature code signals, said link further employed during said operating-receiving mode for transmitting said encoded signal from said transmitter to said access control unit; wherein said control unit is hidden from view within said vehicle at a relatively secure location not visible either from outside the vehicle or from passenger locations within the passenger compartment of said vehicle, and said system further comprises a switch accessible only within said vehicle for selective actuation by the system operator, said control unit being responsive to actuation of said switch for entering the program mode; and further characterized in that said program mode is automatically terminated after a predetermined time delay from receipt of the last transmitted encoded signal.

6. A vehicle security system in which a control unit is responsive to receipt of a proper transmitted encoded radio frequency signal from a transmitter to arm or disarm said system, comprising:

vehicle antitheft means, said means comprising a vehicle ignition disabling means;

a portable hand-held transmitter comprising means for generating and transmitting a predetermined fixed digitally encoded, radio frequency, receiver-responsive signal representative of a predetermined transmitter code; and wherein said predetermined transmitter code comprises a non-user-programmable N-bit digital code word;

a control unit located within said vehicle, comprising:

(i) radio frequency signal receiving means operable during said program mode and during said system operating-receiving mode for receiving said transmitted encoded signal and generating an electrical signal representative of the encoded signal;

(ii) a digital memory for storing signature code signals;

(iii) programming means for recording in said digital memory received signals for arming or disarming said vehicle antitheft means, said means activated only during a system program mode for automatically storing in said memory said electrical signals representative of said radio frequency, receiver-responsive received signals representative of said predetermined transmitter code as a signature code signal for arming or disarming said vehicle antitheft means; and

(iv) operating means activated during an operating-receiving mode for comparing received electrical signals with said signature code signal stored in said memory means to determine if said electrical signals correspond to said recorded signature code signal and for arming or disarming said antitheft means if said electrical signals correspond to said recorded signature code signal, wherein said transmitter and said receiver means cooperate to form a one-way radio frequency signal transmission link for communicating signals only from said transmitter to said receiving means, said transmission link being employed by said system during said programming mode for transmitting said signal representative of said transmitter code to said access control unit to be stored in said memory means as signature code signals, said link further employed during said operating-receiving mode for transmitting said encoded signal from said transmitter to said access control unit.

7. A vehicle security system in which a control unit is responsive to receipt of a proper transmitted encoded radio frequency signal from a transmitter to arm or disarm said system, comprising:

vehicle antitheft means, said means comprising a vehicle ignition disabling means;

a portable hand-held transmitter comprising means for generating and transmitting a predetermined fixed digitally encoded, radio frequency, receiver-responsive signal representative of a predetermined transmitter code;

a control unit located within said vehicle, comprising:

(i) radio frequency signal receiving means operable during said program mode and during said system operating-receiving mode for receiving said transmitted encoded signal and generating an electrical signal representative of the encoded signal;

(ii) a digital memory for storing signature code signals;

(iii) programming means for recording in said digital memory received signals for arming or disarming said vehicle antitheft means, said means activated only during a system program mode for automatically storing in said memory said electrical signals representative of said radio frequency, receiver-responsive received signals representative of said predetermined transmitter code as a signature code signal for arming or disarming said vehicle antitheft means; and

(iv) operating means activated during an operating-receiving mode for comparing received electrical signals with said signature code signal stored in said memory means to determine if said electrical signals correspond to said recorded signature code signal and for arming or disarming said antitheft means if said electrical signals correspond to said recorded signature code signal, wherein said transmitter and said receiver means cooperate to form a one-way radio frequency signal transmission link for communicating signals only from said transmitter to said receiving means, said transmission link being employed by said system during said programming mode for transmitting said signal representative of said transmitter code to said access control unit to be stored in said memory means as signature code signals, said link further employed during said operating-receiving mode for transmitting said encoded signal from said transmitter to said access control unit; further characterized in that said access control unit is operable in the program mode to automatically record a plurality of different transmitter codes from a plurality of different transmitters codes and wherein said control unit is responsive to received signals corresponding to any one of said stored transmitter codes for arming or disarming the vehicle antitheft means; and wherein said transmitter is suitably encoded with said transmitter code by the manufacturer thereof so that the system user is not required to encode said transmitter.

8. A vehicle security system in which a control unit is responsive to receipt of a proper transmitted encoded radio frequency signal from a transmitter to arm or disarm said system, comprising:

vehicle antitheft means, said means comprising a vehicle ignition disabling means;

a portable hand-held transmitter comprising means for generating and transmitting a predetermined fixed digitally encoded, radio frequency, receiver-responsive signal representative of a predetermined transmitter code;

a control unit located within said vehicle, comprising:

(i) radio frequency signal receiving means operable during said program mode and during said system operating-receiving mode for receiving said transmitted encoded signal and generating an electrical signal representative of the encoded signal;

(ii) a digital memory for storing signature code signals;

(iii) programming means for recording in said digital memory received signals for arming or disarming said vehicle antitheft means, said means activated only during a system program mode for automatically storing in said memory said electrical signals representative of said radio frequency, receiver-responsive received signals representative of said predetermined transmitter code as a signature code signal for arming or disarming said vehicle antitheft means; and

(iv) operating means activated during in operating-receiving mode for comparing received electrical signals with said signature code signal stored in said memory means to determine if said electrical signals correspond to said recorded signature code signal and for arming or disarming said antitheft means if said electrical signals correspond to said recorded signature code signal, wherein said transmitter and said receiver means cooperate to form a one-way radio frequency signal transmission link for communicating signals only from said transmitter to said receiving means, said transmission link being employed by said system during said programming mode for transmitting said signal representative of said transmitter code to said access control unit to be stored in said memory means as signature code signals, said link further employed during said operating-receiving mode for transmitting said encoded signal from said transmitter to said access control unit; and wherein said control unit is operable in the program mode to record a plurality of different transmitter encoded signals of different code bit lengths as valid signature code words, and operable in the operating-receive mode to decode and compare said decoded signals of different bit lengths to each of said recorded signature code signals.

9. A vehicle security system in which a control unit is responsive to receipt of a proper transmitted encoded radio frequency signal from a transmitter to arm or disarm said system, comprising:

vehicle antitheft means, said means comprising a vehicle ignition disabling means;

a portable hand-held transmitter comprising means for generating and transmitting a predetermined fixed digitally encoded, radio frequency, receiver-responsive signal representative of a predetermined transmitter code;

a control unit located within said vehicle, comprising:

(i) radio frequency signal receiving means operable during said program mode and during said system operating-receiving mode for receiving said transmitted encoded signal and generating an electrical signal representative of the encoded signal;

(ii) a digital memory for storing signature code signals;

(iii) programming means for recording in said digital memory received signals for arming or disarming said vehicle antitheft means, said means activated only during a system program mode for automatically storing in said memory said electrical signals representative of said radio frequency, receiver-responsive received signals representative of said predetermined transmitter code as a signature code signal for arming or disarming said vehicle antitheft means, and

(iv) operating means activated during an operating-receiving mode for comparing received electrical signals with said signature code signal stored in said memory means to determine if said electrical signals correspond to said recorded signature code signals and for arming or disarming said antitheft means if said electrical signals correspond it said recorded signature code signal, wherein said transmitter and said receiver means cooperate to form a one-way radio frequency signal transmission link for communicating signals only from said transmitter to said receiving means, said transmission link being employed by said system during said programming mode for transmitting said signal representative of said transmitter code to said access control unit to be stored in said memory means as signature code signals, said link further employed during said operating-receiving mode for transmitting said encoded signal from said transmitter to said access control unit; and wherein said transmitter comprises means for selectively generating and transmitting either a first or a second predetermined digitally encoded, radio frequency signal representative of first or second predetermined transmitter codes, said control unit is operable in the program mode to record respective signals representative of said first or second transmitter codes, and wherein said operating means comprises means for arming or disarming said antitheft means in response to receipt of signals corresponding to said first code, and means for performing a second predetermined function in response to signals corresponding to said second transmitter code.

10. An electronically programmable remote control vehicle security system, comprising:

a multi-channel remote control transmitter comprising means for generating a plurality of predetermined digitally encoded, radio frequency, signals representative of a plurality of predetermined transmitter channel signature codes, and user-activated means for selecting and transmitting respective ones of said signals;

vehicle antitheft means;

a system control unit disposed within said vehicle, comprising:

(i) receiving means operable during a system program mode and a system operating-receiving mode for receiving said transmitted encoded signal and generating an electrical signal representative of the encoded signal;

(ii) a digital memory for storing data representative of signature code signals, said memory comprising a plurality of assigned memory locations for storing signature code signals for each of said channels;

(iii) programming means activated only during said system program mode for selecting a particular channel and storing in an assigned memory location in said memory received signals representative of said predetermined transmitter channel code as a signature channel control signal;

(iv) operating means activated during said operating-receiving mode for comparing received electrical signals with said signature control signals stored in said memory means to determine if said electrical signals correspond to said recorded signature code signal, means for determining the channel having a corresponding signature channel control signal stored therein, and responsive action means for the respective identified channel activated upon receipt of a matching channel signature code;

wherein said transmitter and said receiving means cooperate to form a one-way radio frequency signal transmission link for communicating signals only from said transmitter to said receiving means, said transmission link being employed by said system during said programming mode for transmitting said encoded signals from said transmitter to said access control unit to be stored in said memory as said code signals, said link further employed during said operating receiving mode for transmitting said encoded signals from said transmitter to said control unit; and wherein said transmitter is suitably encoded with said predetermined transmitter code by the manufacturer thereof so that the system user is not required to encode said transmitter.

* * * * *

US005650774A

United States Patent [19]

Drori

[11] Patent Number: 5,650,774

[45] Date of Patent: *Jul. 22, 1997

[54] ELECTRONICALLY PROGRAMMABLE REMOTE CONTROL ACCESS SYSTEM

[75] Inventor: Ze'ev Drori, Chatsworth, Calif.

[73] Assignee: Clifford Electronics, Inc., Chatsworth, Calif.

[*] Notice: The term of this patent shall not extend beyond the expiration date of Pat. No. 5,146,215.

[21] Appl. No.: 334,843

[22] Filed: Nov. 4, 1994

Related U.S. Application Data

[63] Continuation of Ser. No. 118,167, Sep. 8, 1993, abandoned, which is a continuation of Ser. No. 944,038, Sep. 11, 1992, abandoned, which is a continuation of Ser. No. 719,095, Jun. 20, 1991, abandoned, which is a continuation of Ser. No. 555,357, Jul. 17, 1990, abandoned, which is a continuation of Ser. No. 406,837, Sep. 13, 1989, abandoned, which is a continuation of Ser. No. 94,395, Sep. 8, 1987, abandoned.

[51] Int. Cl.[6] G06F 7/04

[52] U.S. Cl. 340/825.32; 340/825.31; 340/825.69; 340/825.72

[58] Field of Search 307/10.2; 70/278; 340/528, 541, 543, 542, 825.31, 825.32, 825.69, 825.71; 361/172

[56] **References Cited**

U.S. PATENT DOCUMENTS

3,337,992	8/1967	Tolson	49/29
4,148,012	4/1979	Baump et al.	340/149
4,177,657	12/1979	Aydin	70/219
4,236,068	11/1980	Walton	235/380
4,245,212	1/1981	Cirimele	340/147
4,383,242	5/1983	Sassover et al.	340/64
4,525,805	7/1985	Prosan et al.	364/900
4,535,333	8/1985	Twardowski	340/825.72
4,573,046	2/1986	Pinnow	340/825.56
4,626,848	12/1986	Ehlers	340/825.72
4,652,860	3/1987	Weishaupt et al.	340/825.31
4,665,397	5/1987	Pinnow	340/825.72
4,750,118	6/1988	Heitschel et al.	340/825.69
4,754,255	6/1988	Sanders et al.	340/64
5,146,215	9/1992	Drori	340/825.32

FOREIGN PATENT DOCUMENTS

WO-A-8501980	5/1985	European Pat. Off. .
0139059	5/1985	European Pat. Off. .
0162171	11/1985	European Pat. Off. .
0306598	3/1989	European Pat. Off. .
2580128	10/1986	France .
2116808	9/1983	United Kingdom .

OTHER PUBLICATIONS

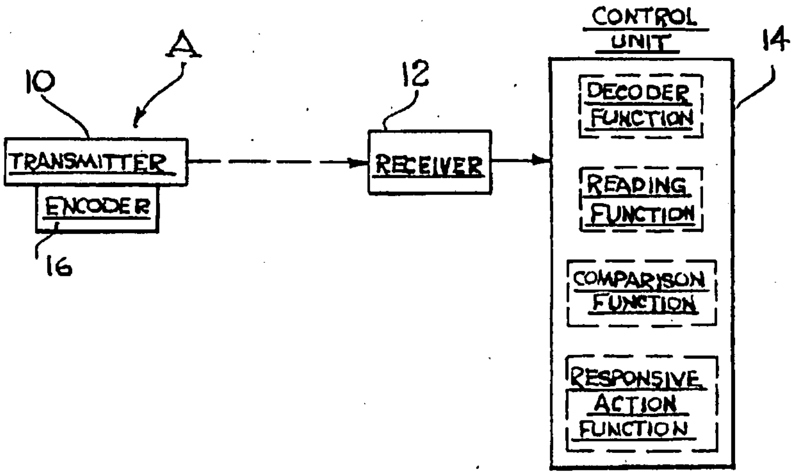
Translation Document Re French Patent 2.580.128.

Primary Examiner—Regina D. Liang

[57] **ABSTRACT**

A remote control access system which may be in the form of a security system or a convenience system for buildings and vehicles to thereby enable access opening and closing of buildings and vehicles. The system is operable on a remote control basis and comprises one or more hand held remote transmitters and a receiver unit located at or near the building or in the vehicle. The receiver is operable in conjunction with a control unit which contains a microprocessor capable of performing control functions and decoding functions. The remote control access system is unique in that it enables the user to electronically program into or delete from the receiver a digital code or so-called encoding signal from any of a plurality of transmitters. Each transmitter may contain not only different numbers of digital codes, but also a code generated by an entirely different method of encoding. Moreover, it is not necessary for the user or anyone else to know the specific encoded signal which is transmitted from any of the transmitters to the receiver. The receiver is operable with a plurality of transmitters, all of which operate on the same frequency. The present invention also provides an anti-sequencing capability such that one cannot use an electronic sequencer for detecting the code of the transmitter for purposes of violating the security system.

15 Claims, 4 Drawing Sheets



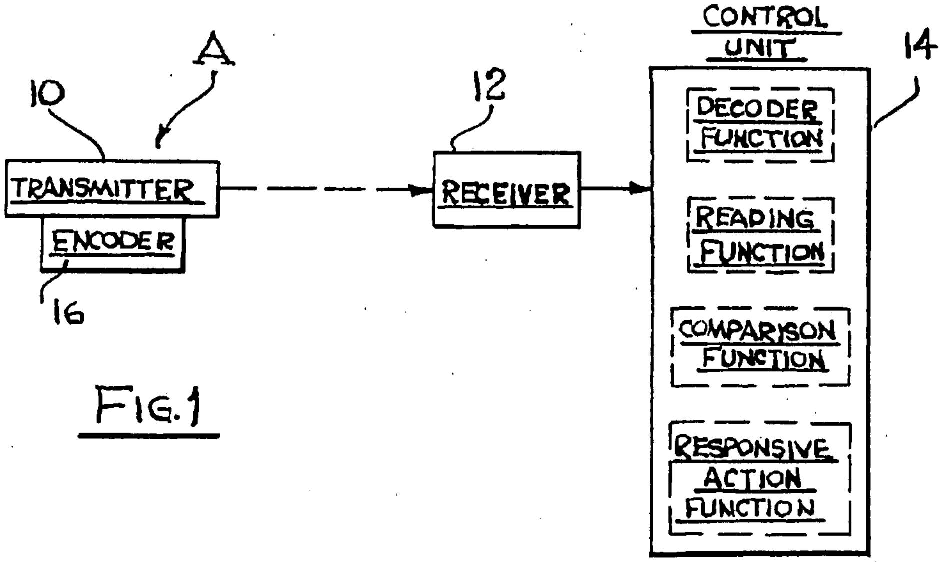

CONTROL UNIT
14
A
10
12
DECODER FUNCTION
TRANSMITTER
RECEIVER
READING FUNCTION
ENCODER
16
COMPARISON FUNCTION
RESPONSIVE ACTION FUNCTION

FIG. 1

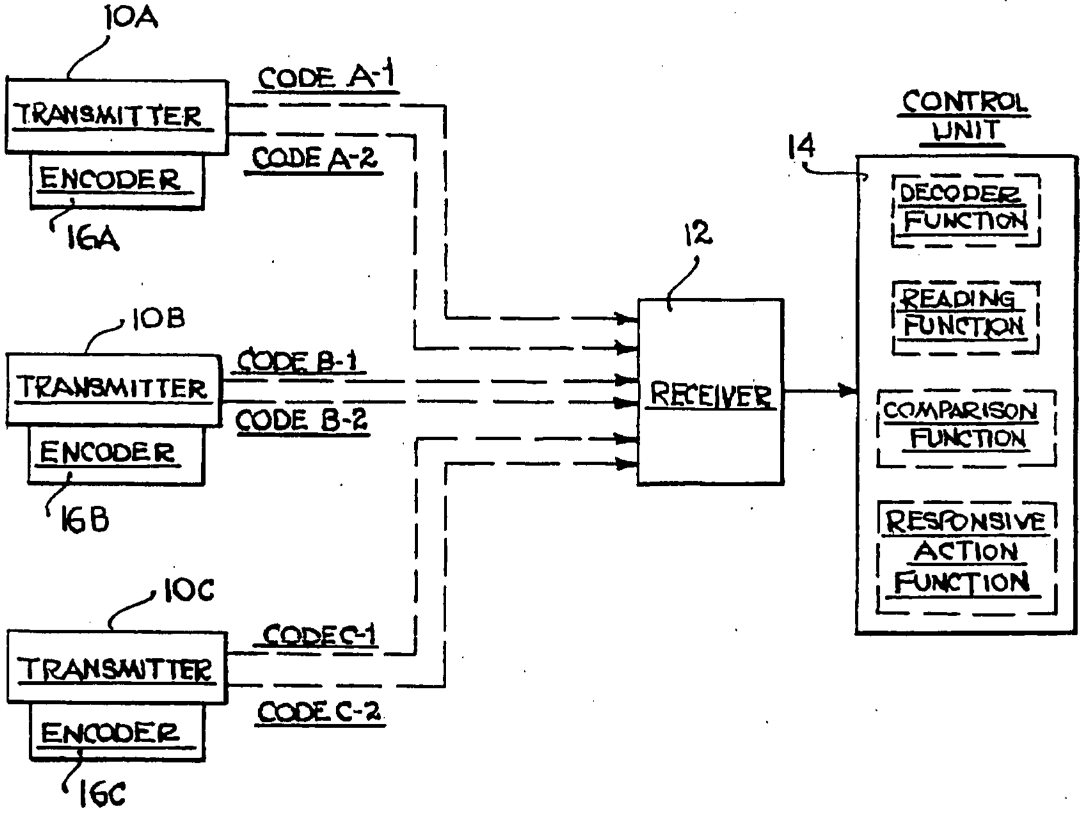
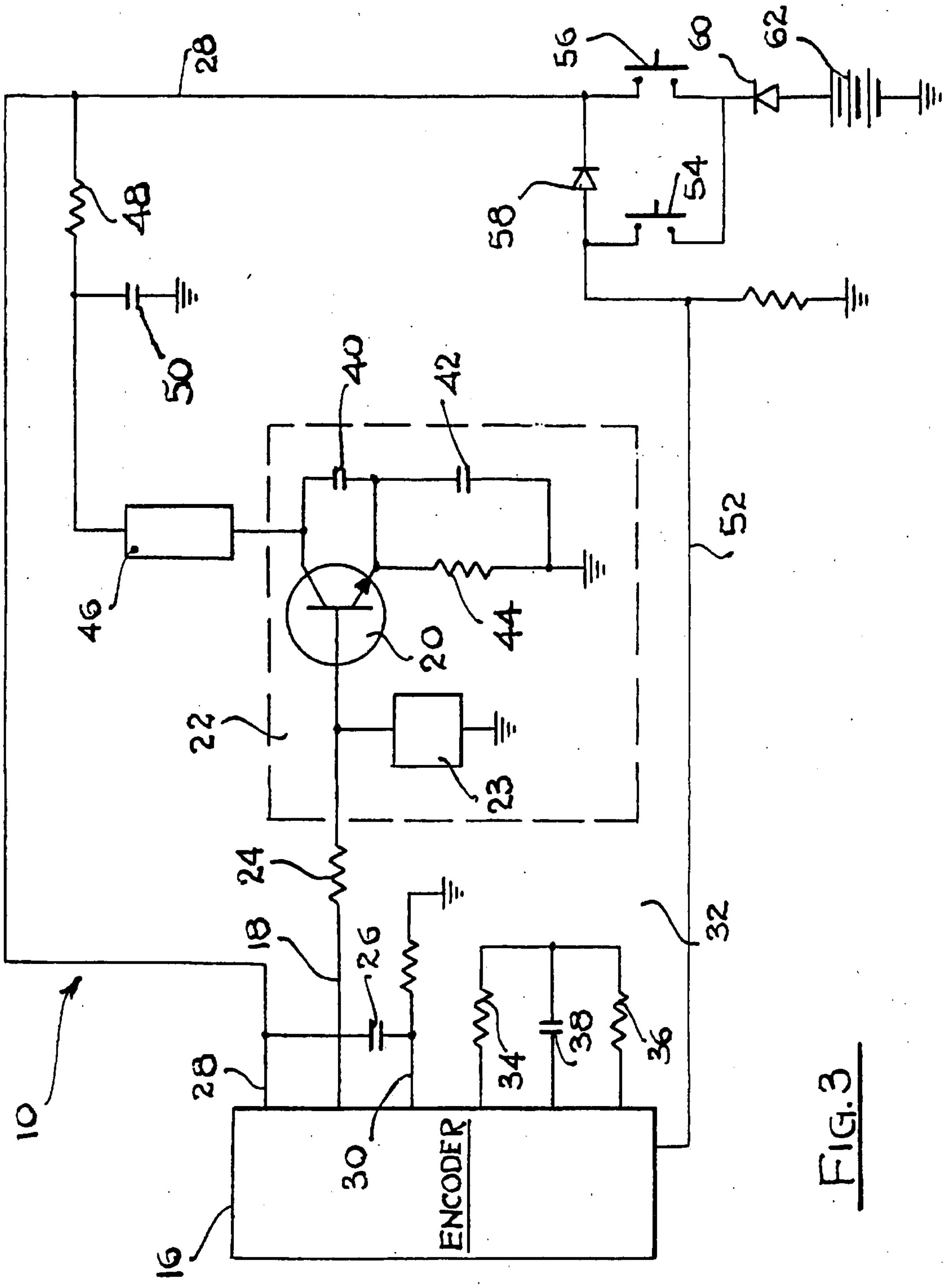

10A
TRANSMITTER
CODE A-1
CODE A-2
ENCODER
16A
CONTROL UNIT
14
DECODER FUNCTION
12
READING FUNCTION
10B
TRANSMITTER
CODE B-1
CODE B-2
RECEIVER
ENCODER
16B
COMPARISON FUNCTION
RESPONSIVE ACTION FUNCTION
10C
TRANSMITTER
CODE C-1
CODE C-2
ENCODER
16C

FIG. 2



28
56
60
62
54
58
48
50
40
42
52
46
20
44
22
23
24
18
26
32
34
38
36
28
10
30
ENCODER
16

FIG. 3

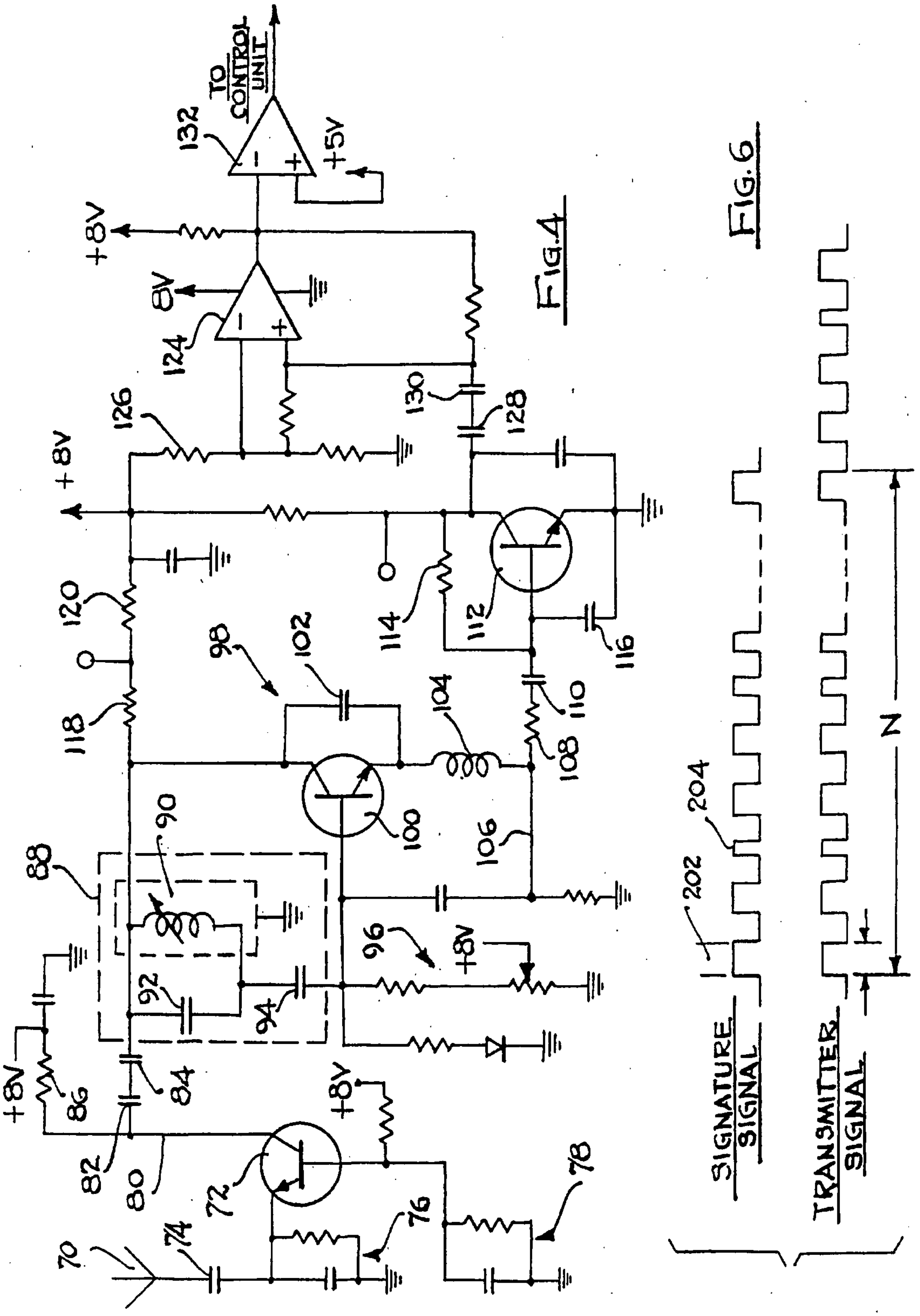

TO CONTROL UNIT
132
+5V
+8V
8V
124
126
+8V
130
128
120
118
98
102
114
112
116
104
110
108
88
90
100
106
92
94
96
+8V
+8V
86
84
82
80
+8V
72
78
76
74
70
202
204
N
SIGNATURE SIGNAL
TRANSMITTER SIGNAL

FIG. 4

FIG. 6

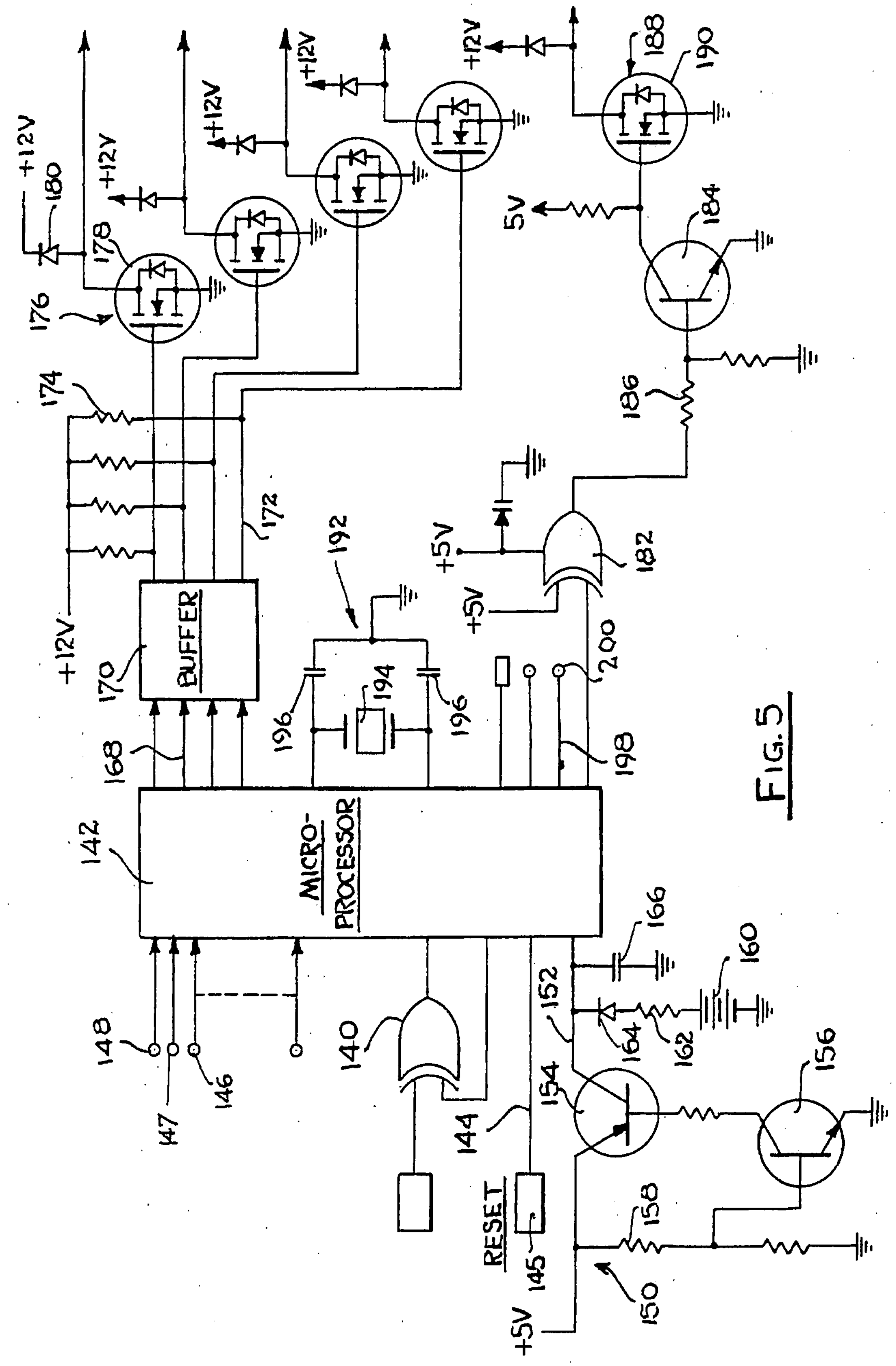

BUFFER
MICRO-PROCESSOR
RESET
+12V
+5V
5V
142
144
145
146
147
148
150
152
154
156
158
160
162
164
166
168
170
172
174
176
178
180
182
184
186
188
190
192
194
196
198
200

FIG. 5

ELECTRONICALLY PROGRAMMABLE REMOTE CONTROL ACCESS SYSTEM

This is a continuation of application Ser. No. 08/118,167 filed on Sept. 8, 1993 now abandoned, which is continuation of Ser. No. 07/944,038 filed on Sept. 11, 1992 abandoned, which is continuation of Ser. No. 07/719,095 filed on Jun. 20, 1991, abandoned, which is continuation of Ser. No. 07/555,357 filed on Jul. 17, 1990, abandoned, which is continuation of Ser. No. 07/406,837 filed on Sept. 13, 1989, abandoned, which is continuation of Ser. No. 07/094,395 filed on Sept. 8, 1987, now abandoned.

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates in general to certain new and useful improvements in remote control access systems, and more particularly, to remote control access systems which are comprised of a receiver-control unit located at or near an enclosed environment, and one or more remote transmitters, and which systems are electronically programmable by any user without knowledge of the specific code used or operation of the system itself.

2. Brief Description of the Prior Art

Remote control systems are widely used in a large number of applications in which a receiver is located to control some type of electronic equipment and which is operable by one or more remotely located transmitters. Usually, these receiver-transmitter arrangements are radio frequency operated, although they can be operated with other forms of electromagnetic radiation or sound energy.

The remote control access systems may adopt the form of convenience systems such as garage door openers which control the opening and closing of a garage door, as well as security systems such as those providing controlled entry into vehicles and buildings. The area which is to be secured by the remote control access system is often referred to as "protected environment" or the "secured environment."

In recent years, and primarily due to the increase of theft, vandalism and burglaries, many home and vehicle owners have installed remote access control systems, such as security systems and remote controlled garage door systems. The vast majority of these security systems, when triggered, will generate an audible or visible alarm signal or otherwise a silent alarm signal transmitted to a security force, such as a police department to alert of an improper entry or an improper intrusion into the protected area. Many of these commercially available security systems are remotely operable, that is, they include a receiver capable of being operated from a remotely located transmitter for purposes of arming and dis-arming the security system.

The present state of the art in conventional automotive vehicle security systems usually includes an alarm section which may either generate an audible alarm, as for example, from a siren, a horn, or the like and may also often activate a visible alarm by operating any of the vehicle lights. Many of these commercially available vehicle security systems may also disable some portion of the vehicle engine system such as the ignition system, starter, fuel pump, or lock the engine compartment. Thus, in the event of an improper intrusion or attempted theft of the vehicle, the security system will cause initiation of an audible alarm or cause the lights to switch on and off and may also interfere with operation of the vehicle engine system.

The use of a transmitter and a receiver which have been pre-coded is generally standard with all commercially available remote control access systems and other remote control systems. In these transmitter-receiver combinations, the code, usually referred to as an encoded signal, is permanently encoded into the receiver.

In the remote control security systems, the transmitter is always pre-programmed with respect to the receiver and the code can't be altered or changed by the user. In other words, the receiver can only operate on the basis of a security code permanently encoded in that receiver and transmitted from a particular transmitter matched and sold with that receiver.

In addition to being quite limiting to and having a security exposure in case of a loss or stolen transmitter they also present many constraints on the manufacturers, customers and dealers of these security systems. For instance, if the user of one of these prior art security systems should lose his or her transmitter, it is necessary to obtain another transmitter which was not previously coded and have that transmitter properly matched and coded for the particular receiver.

The encoding of the transmitter entails, at very least, obtaining the particular code to introduce into the transmitter for activating the receiver. This encoding also includes the requirements of opening the transmitter and then mechanically coding the transmitter. Usually, the coding is accomplished by scratching conductive lines on a printed circuit board, closing or opening switches or the like. Some transmitters are provided with control boards having hole areas capable of being punched to provide a particular encoded signal. In any event, some form of mechanical action is usually required for encoding the transmitter after the latter has been opened.

Usually, most users of the remote control access systems are not capable of encoding the transmitters on their own, and therefore, must seek the assistance of the retailer or manufacturer of the system. The mere fact that the code for authorized actuation of the security system must be known by the selling dealer or manufacturer may inevitably lead to a breach of the security system itself, since the code is usually written to maintain a permanent record of the same. More importantly should the user wish to change the code because of a lost or stolen transmitter, both the transmitter and the receiver will have to be sent back to the manufacturer. This is a time consuming task which leaves the user without the security system, in addition to being costly.

In addition to the foregoing, if a user desires to have several transmitters operate the receivers of several remote control access systems, such as security systems or garage door systems, each receiver must be properly programmed with the proper code. As an example, if a person desired to operate, with the same remote control system, several vehicles and garage doors, it is necessary to have a receiver in each car and a receiver in each garage door system pre-programmed by a manufacturer. This necessarily requires custom design efforts which is very time consuming as well as costly.

Since most security systems and remote garage door openers operate with substantially less than one million code combinations it has been recently recognized that many commercially available electronic sequencing devices (often referred to as "electronic scanners") can, in effect, remotely decode that security code in a fairly short period of time. The electronic sequencers or scanners are capable of rapidly generating a large number of possible code combinations and when the right code combination has been generated, it will automatically disarm the security system. There is not any decoding-proof measure which is commercially available for preventing anyone from using an electronic sequencing apparatus to disarm a security system.

OBJECTS OF THE INVENTION

It is, therefore, one of the primary objects of the present invention to provide a radio frequency operated remote control system in which the receiver of the system can be electronically programmed by the user of the system without opening the transmitter, and without coding the transmitter or changing or encoding the receiver or acquiring dealer or manufacturer assistance.

It is another object of the present invention to provide a remote control system of the type stated in which neither the manufacturer, dealer or user of the system are required to know the particular code which is transmitted from the transmitter to the receiver.

It is a further object of the present invention to provide a method for a user of a remote control system to encode a receiver from a transmitter without any prerequisite skill or the need to even open the case of neither the transmitter nor the receiver.

It is also an object of the present invention to provide a remote control system of the type stated which does not require the provision of a separate decoder along with the receiver.

It is an additional object of the present invention to provide a remote control system of the type stated where completely different types of transmitters may be provided and where each transmitter may control totally different areas and they may operate with totally different numbers of possible codes.

It is yet another object of the present invention to provide a remote control system of the type stated where any of a multiplicity of transmitters may be added to or deleted from the system at will by the user.

It is still another object of the present invention to provide a remote control system of the type stated where each transmitter may be programmed to a different priority level, thereby enabling an accessing or controlling to pre-assigned functions.

It is still a further object of the present invention to provide a remote control system of the type stated which may be provided with an anti-scanning feature to preclude electronic scanning and unauthorized disarming of the system.

It is another salient object of the present invention to provide a remote control system of the type stated which can produce multi-billion codes thereby providing code security of at least two thousand times the code security of prior art systems and yet which can be manufactured at a relatively low cost.

With the above and other objects in view, my invention resides in the novel features of form, construction, arrangement, and combination of parts presently described and pointed out in the claims.

BRIEF SUMMARY OF THE INVENTION

A remote control access system which is comprised of at least one receiver connected to electronic or electrical equipment which will enable or perform various functions when activated and one or more transmitters which can actuate the receiver by generation of a code or encoded signal. As an example, one of the functions which may be enabled or performed is that of controlling an access opening. The receiver is operable with a control unit and this control unit is preferably a microprocessor control unit in accordance with the present invention. Moreover, the receiver and microprocessor control unit can perform all of the necessary decoding functions.

In one embodiment of the invention, one or more transmitters forming part of the system may have the provision of an encoder included therein. The one or more encoders will generate encoded signals upon actuation of the transmitters. This embodiment of the invention also comprises a receiver-control unit at the secured or protected environment, and is responsive to the encoded signal and enables operation of an access system.

The control unit is operable with the receiver at a protected or access controlled environment, and which is preferably a microprocessor operated control unit, as aforesaid. The control unit performs several primary functions including a decoding function. Thus, when the receiver receives the encoded signal, the microprocessor validates and decodes the transmitted signal. Thus, there is no requirement for the provision of a separate decoder in the protected environment.

The remote control access system of the present invention is also highly effective in that it is electronically user programmable. In effect, the receiver can be programmed by the user at any time. Moreover, no tooling or skills are required on the part of the user in order to program the receiver. The user is not even required to open the transmitter case or receiver housings when programming the system. The user of the system may initiate the receiver's program mode at any time so that it will enable recording and thereby enable recognition of subsequent messages or encoded signals from the transmitter. This may be accomplished by activating a record switch in the receiver, either mechanically, electronically or through voice recognition. Thereafter, the user actuates the transmitter, as for example, by pressing a switch on the transmitter. This will cause the encoded signal generated by the encoder to be transmitted by the transmitter to the receiver.

The receiver and control unit will operate to decode the transmitted signal and which decoded signal is then programmed into a memory unit, as hereinafter described, and becomes the control signal or so-called "signature control signal". In this sense, the system of the present invention is user programmable. Moreover, it is not necessary for anyone to know the specific encoded signal which is in the control unit, initially, or at any time thereafter. The control unit will, in effect, have received the signature of the transmitter and will record that signature in the random access memory of the microprocessor.

The receiver-control unit may be arranged so as to automatically exit the signature signal record mode after recording thereof. This automatic exit may occur for example, after a certain time delay in which no further signal has been received. Otherwise, the receiver may be arranged so that it is manually switched by the user out of the signature signal record-mode or so-called "program mode."

The receiver-control unit in the system of the present invention may also be operated by several transmitters, and each of which may be used to operate the receiver and control unit. Each transmitter may operate with a completely different code or encoded signal than any of the other transmitters and in this case, the receiver will be responsive to each transmitter which has its code or encoded signal recorded in the control unit as a signature control signal. It is not even necessary for the transmitters to be of the same type.

Each transmitter may have a totally different maximum number of digital code combinations. For example, one transmitter may have a ten-bit code and therefore, is able to produce one thousand twenty-four possible combinations of unique codes. Yet another transmitter may operate with a thirty-two bit code, thus possessing more than four billion possible digital codes. The construction and the operation of these transmitters may be different and each may have a different number of switches and/or codes, as aforesaid. However, it is important that each transmitter operate on the same frequency as the receiver.

In accordance with the above if a plurality of individuals are required to have access to the arming and dis-arming of the system, each may be provided with the same or different transmitters. Each such individual will initially operate his or her transmitter to record the signature of that transmitter in the random access memory of the microprocessor, as one of the control signals or signature control signals. After this has been accomplished, each party using any one of the transmitters, whose signatures have been recorded, may then access the system by either arming or dis-arming the system, or enabling specific functions assigned only to one or more specific transmitters. Moreover, the system may be armed by one transmitter and disarmed by a second transmitter, re-armed by a third transmitter, and disarmed by a fourth transmitter, etc.

Any one of the transmitters may also be programmed out of the system, that is deleted from the system, by first entering the recording or program mode, and then programming repeatedly, the rest of the transmitters until the memory of the control unit is fully loaded.

In the event that any particular transmitter is lost or stolen, it is only necessary to erase the recorded signature control signals in the memory and re-record the signature control signals from the other transmitters which have not been lost or stolen. In this way, anyone who attempts to use the lost or stolen transmitter will not be able to arm or dis-arm the remote control access system. There is essentially no breach in security inasmuch as one must have access to the receiver-control unit which is generally located in the secured environment.

The remote-control access system of the present invention may assign different access or controlling functions to different transmitters. As an example, one transmitter may have access to a first portion of a secured environment, a second transmitter may have access to a second portion of a secured environment, etc. In like manner, one transmitter may have access to a first portion of a secured environment and a second transmitter may have access to that first portion and another portion of a secured environment. In this way the arrangement is highly effective for controlling parties having access to classified information. Thus, one party having access to a lower level of classified information will have access to an area containing that information. Another party having access to an intermediate level of classified information will have access to the areas containing the lower level of classified information and the area containing the intermediate levels of classified information. Parties having access to a high security level of information as for example, a "top secret" level of information will have access to all levels of information.

The arrangement for controlling access to different areas of a secured environment is easily accomplished with the system of the present invention. It is only necessary to record the signature control signals from those transmitters into receiver-control units which are designed to enable access to certain areas. Thus, a transmitter which is designed to provide access to a first secured area will have its signature control signal encoded in the receiver-control unit at the access opening of that first area. A transmitter permitting access to a second secured area will have its signature control signal recorded in the receiver-control unit located to control the access opening to both the first secured area and the second secured area.

In still another embodiment of the present invention, the remote control system may be provided with an anti-scanning feature. The anti-scanning feature prevents a so-called "breaking" of the encoded signal. Heretofore, it was possible, in a given time frame, to generate a large number of coded signals and essentially all possible combinations thereof, for example 16,000 possible combinations with an electronic scanner. The present invention will preclude the arming or dis-arming of the security system by the prior art scanning procedures.

The microprocessor is constructed, in this embodiment of the invention, to operate in such manner that it will not permit arming or disarming of the system for a predetermined time period in the event of the receipt of an unauthorized or invalid encoded signal, as for example, a four-second delay. Thus, a typical scanner which generates coded signals on a rapid basis, usually much faster than the time delay period, will attempt to transmit a large number of coded signals in a short time frame to the receiver in the anticipation that one of the coded signals would arm or dis-arm the system. However, on each occasion that the the control unit detects an improper or invalid coded signal, the time delay is continued. Thus, if a first encoded signal is an invalid code or an unauthorized signal, the control unit will not permit operation of the security system for a pre-set time delay. If any successive encoded signal is also an invalid code or an unauthorized signal, then the pre-set time delay is continued for an additional pre-set time delay increment and so forth. The disabling time of the decoder in response to each invalid code is longer than the time it takes to generate a code by the scanner's encoder. Thus, even when a valid code is transmitted, it will not deactivate the system since it was preceeded by an invalid code. In this way, a conventional scanning device could not generate the proper coded signal in a time domain necessary to arm or disarm the security system.

The microprocessor operated control unit also performs a reading function and a comparison function. In the reading operation, the control unit will read two or more successive and sequentially transmitted and decoded signals and will recognize them as correctly (authorized—not necessarily valid) transmitted signals, if two or more successive transmitted signals correspond. In this way, the control unit can determine if there is an error in transmission.

In the comparison function, the control unit will read a transmitted and decoded signal which is often referred to as a "received signal", and then compare that transmitted and decoded signal to a stored code or stored encoded signal which has been previously stored in the random access memory of the processor. Thus, and in this respect, the microprocessor operated control unit will perform a comparison function. This stored signal is typically referred to as a "control signal" or a "signature signal" since it is, in effect, the signature signal transmitted from the transmitter.

In the comparison operation, if the encoded signal which has been received and decoded corresponds to a previously recorded signal or signature signal, then the control unit will recognize the received decoded signal as a valid signal. Contrarywise, if the received and decoded signal does not correspond a previously recorded signature signal, the microprocessor will recognize that received and decoded signal as an invalid and unathorized signal and will not enable a disarming of the security system.

If the signal which has been decoded and compared does correspond to a previously recorded signal and is thereby a valid signal, then the microprocessor will either enable or disable or initiate various commands. For example, if the security system was armed when the valid decoded signal was received, then the microprocessor will enable a disarming of the system. If the system was dis-armed when the valid decoded signal is received, then the microprocessor will enable an arming of the security system.

The term "signal", and particularly with reference to an encoded transmitted signal or a received and decoded signal, is used in a general sense to refer to a transmitted or received code which may be comprised of a plurality of bits and/or bytes of information. Thus, as a simple example, in one of the embodiments of the system of the present invention, the encoded signal may be comprised of eighteen bits of information.

In view of the above, it can be observed that among the very significant advantages offered by the remote control security system of the present invention are the following:

1) The security system is self-programmable by a user at any time in such manner as the user can merely actuate a switch-type element on the receiver and press a button on the transmitter for automatically programming a selected code into the receiver as a signature control signal.

2) A signature control signal may be eliminated from the receiver-control unit by recording the codes of the desired transmitters several times until the memory of the control unit is fully loaded.

3) It is not necessary for any one to know the code for triggering of the remote control system inasmuch as any code already programmed in the remote control transmitter will be automatically recorded into the memory of the receiver-control unit when the receiver-control unit is in the program mode and the remotely located transmitter is activated.

4) The security level of the present invention can be upgraded by the user at any time, as for example, by utilizing upgraded transmitters with a substantially greater number of digital codes, or the like, and which is virtually impossible in any of the prior art remote control security systems. In this way, for example, the remote control system can be upgraded by the owner, at will, from 16,000 combinations of digital codes to over 4 billion digital code combinations without modifying or installing a new system.

5) In reading the encoded signal transmitted from the transmitter, a reading operation is conducted by the control unit associated with the receiver on two consecutive received signals to ensure that there is no error in the received signals before determining if that received and decoded signal compares to the signature control signal.

6) The transmitter and receiver are uniquely designed so that neither has to be opened and electronic or mechanical knowledge is not required for installing a new encoded signal at any time.

7) The remote control access system of the invention can operate with numerous types of transmitters, so long as they essentially operate at the same frequency range. This enables the purchase of transmitters from a source different from the receiver and control unit.

8) The remote control access system of the invention can operate by controlling access to different areas of a secured environment with different transmitters. Thus, one transmitter may provide access to a first portion of a secured area and a second transmitter may provide access to a second portion of a secured area.

9) The remote control security system of the present invention possesses an anti-scanning feature that makes it virtually impossible to determine the encoded signal by electronic scanning.

10) The remote control system of the invention also uses significantly fewer electronic components than the prior art systems, and as an example, a decoder is not required inasmuch as the microprocessor can perform the decoding function.

The above identified advantages are only a non-limiting list, but include some of the significant advantages which are achieved by the system of the present invention.

In one of the preferred environments of the invention, the remote control access system of the invention is used in conjunction with or forms part of a security system, as for example, an automotive vehicle security system. Although the invention is not so limited, the remote controlled system of the invention will be described in connection with and as a part of an automotive vehicle security system.

While the remote control access system of the present invention has been designed for use with vehicles, and more specifically, for use with automotive vehicles, the security system can be used with essentially any form of vehicle, including airplanes, boats, trucks, and the like. Moreover, the security system is highly effective for use in buildings, including dwelling structures, office buildings, garages and the like. Thus, with little or no modification, the access system is capable of being used in a wide variety of environments and is therefore highly versatile.

This invention possesses many other advantages and has other purposes which may be made more clearly apparent from a consideration of the forms in which it may be embodied. These forms are shown in the drawings accompanying and forming part of the present specification. They will now be described in detail for purposes of illustrating the general principles of the invention, but it is to be understood that such detailed description is not to be taken in a limiting sense.

BRIEF DESCRIPTION OF THE DRAWINGS

Having thus described the invention in general terms, reference will now be made to the accompanying drawings (four sheets) in which:

FIG. 1 is a block diagram of the major components of a remote control security system constructed in accordance with and embodying the present invention;

FIG. 2 is a block diagram of a modified form of the remote control security system constructed in accordance with and embodying the present invention;

FIG. 3 is a schematic electronic circuit view showing a portion of the transmitter forming part of a remote control security system of the present invention constructed in accordance with and embodying the present invention;

FIG. 4 is a schematic electronic circuit view showing one embodiment of a receiver forming part of a remote control security system constructed in accordance with and embodying the present invention;

FIG. 5 is a schematic electronic circuit view showing the control unit forming part of the remote control security system constructed in accordance with and embodying the present invention; and

FIG. 6 is a timing diagram of a plurality of wave forms showing a transmitted encoded signal.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

Referring now in more detail and by reference characters to the drawings which illustrate practical embodiments of the present invention. A designates a remote control system in the form of a remote control security system. As indicated previously, a security system is only one form of an access control system which controls the access into buildings or vehicles or like environments. However, since the remote control system of the invention finds a preferred use in security systems, it will be described in connection with a remote controlled security system, although it is to be understood that the invention is not so limited.

The security system is comprised of a transmitter unit **10**, a receiver **12**, and a microprocessor based control unit **14**. The transmitter **10** is schematically shown as including an encoder **16** forming a part thereof. Moveover, the control unit is shown with various functions which may be performed therein or in conjunction therewith. As an example, these functions may be performed by programming various steps into the microprocessor, or otherwise, they could be performed by discrete apparatus carrying out the functions as identified but which would operate in conjunction with the control unit **14**.

FIG. **3** illustrates one embodiment of a transmitter unit which may be constructed in accordance with and embodying the present invention. However, inasmuch as numerous transmitters may be used in accordance with the present invention, as previously described, this particular embodiment of the transmitter is only one of the preferred embodiments, although other electrical circuit arrangements could be employed with the transmitter.

The transmitter **10** generally comprises the encoder **16**, as aforesaid, and which may be suitably encoded by the manufacturer so that the user is not required to encode the same. For this purpose, small switches may be provided on the encoder, or other means known in the art, could be provided on the encoder for specifically generating an encoded signal. A plurality of output lines **18** extend from the encoder **16** in the manner as illustrated in FIG. **3**. One such output an line **18** is connected to an NPN transistor **20** forming part of an oscillator transmitter **22**, as illustrated by the dotted lines in FIG. **3**. The conductor **18** is actually connected to the base of the transistor **20**, as shown. The conductor **18** is also connected through a resonator **23** which is in turn, grounded. A resistor **24** is located in the conductor **18** and serves as a current limiter due to the fact that the transistor **20** is a low impedance device.

A capacitor **26** is connected across an additional pair of conductors **28** and **30**, in the manner as shown, and which operates as a reset circuit. This ensures that the encoder will start the generation of each new encoded signal when actuated on each occasion.

In addition, a resistive-capacitive network **32** is also connected to the output of the encoder **16** in the manner as shown in FIG. **3**, and comprises a pair of resistors **34** and **36** and a capacitor **38**. This circuit arrangement stabilizes the length of each of the bits which are generated by the encoder **16**. This is important in connection with the present invention in that the receiver and the control unit may measure the lengths of the bits in order to determine the status of these bits, that is, whether they are a "1" or a "0".

The transistor **20** has a capacitor **40** connected across its emitter and collector in the manner as shown, and an additional capacitor **42** is connected to a resistor **44** on the emitter of the transistor **20**. The capacitors **40** and **42** are generally provided for load matching purposes and the resistor **44** provides a control bias to the transistor **20**.

Connected to the collector of the transistor **20** is a load circuit **46**, as for example, a portion of an antenna load. This load circuit **46** is connected through a resistor **48** to the output conductor **28** of the encoder in the manner as shown. A capacitor **50** is also connected to the load circuit **46** and is grounded. In effect, the point where the capacitor is connected to the load circuit, represents a ground level value. The resistor **48** and the capacitor **50** operate to de-couple a battery as hereinafter described.

Also connected to the conductor **28** and to an additional conductor **52** are a pair of manually operable switches **54** and **56**. These switches **54** and **56** are operable for providing two channels to the encoder. Thus, one of the switches, when actuated, will cause the generation of a first encoded signal. The other of the switches **56**, when actuated, will cause the generation of a second encoded signal. It should also be observed that a diode **58** is connected across the switches **54** and **56**, in the manner as illustrated, and a diode **60** is also connected between the switchs **54** and **56** and a battery **62**.

As indicated previously, the transmitter, as illustrated, is a two-channel transmitter, which is highly preferable in accordance with the present invention. In this way, two individual encoded signals could be generated by actuation of each of the switches **54** and **56** as aforesaid. However, it should also be understood that a single channel encoder could be used. Moreover, various multiple channel encoders, such as, for example, a three-channel encoder or a four-channel encoder, etc. could be employed with slight modification of the circuitry as described herein.

When any one of the switches **54** or **56** are closed, they will complete a circuit to the encoder **16**, causing generation of an electrical signal over the conductor **18** and which is, in turn, transmitted as a radio frequency signal, via the load **46** to the receiver **12**.

The receiver **12** is more fully illustrated in FIG. **4** of the drawings and generally comprises an antenna **70** for picking-up the transmitted signals and which are introduced into an NPN input-matched impedence transistor **72** which matches the impedence of the antenna **70**. This transistor **72** operates as a radio frequency pre-amplifier. A capacitor **74** between the antenna **70** and the pre-amplifier operates as a coupling capacitor. A resistive-capacitive network **76** is connected to the emitter of the transistor-pre-amplifier **72**. Moreover, a second resistive-capacitive network **78** is also connected to the base of the transistor-pre-amplifier **72**.

The collector of the transistor-pre-amplifier **72** is connected to an output conductor **80** which includes a pair of coupling capacitors **82** and **84**. Moreover, an 8-volt power supply is connected to the collector of the resistor-pre-amplifier **72** through a resisitor **86** which isolates the transistor **72** from the power supply and also from the load.

The conductor **80** is connected to a tank circuit **88** through the coupling resistors **82** and **84** and which comprises a variable inductive device **90** provided for adjusting the frequency of the receiver to the transmitter. A capacitor **92** couples one end of the inductive device **90** to the conductor **80**. That same end of the inductive device **90** is also connected through a coupling capacitor **94** to a variable resistor **96**, in the manner as illustrated in FIG. **3**. The variable resistor **96** is also connected to an 8-volt power source.

The conductor **80** is also connected to a local oscillator **98** which includes an NPN transistor **100** and a capacitor **102** connected across the collector end emitter of the transistor **100**. The base of the transistor **100** is similarly connected to the voltage source through the resistor **96**. Moreover, the emitter of the transistor **100** is connected to another inductor **104**, in the manner as illustrated. This arrangement of the local oscillator including the transistor 100, the capacitor 102 and the inductor 104 is designed to detect the pulses included in the signal.

The output of the inductor 104 is connected to another conductor 106 which carries the detected signal. This conductor 106 serves as the main conductor for the pulses which are generated from the signal received from the transmitter. The detected signal pulses are passed through a resistor 108 and a capacitor 110 and to a signal amplifier 112 in the form of an NPN transistor. Another resistor 114 is connected across the collector and the base of the transistor 112. Moreover, the emitter is grounded and is also connected to a coupling capacitor 116.

The collector of the transistor 100 is also connected to a pair of load resistors 118 and 120, in the manner as illustrated in FIG. 4. In addition, a de-coupling capacitor is also connected to the conductor 80 in the manner as illustrated. Further, an 8-volt power supply is connected through a load resistor 122 to the collector of the transistor 112. At the point where the 8-volt power supply is connected to the conductor 80, a DC voltage is available. Moreover, this DC voltage may be applied to a comparator 124 through a resistor 126. Moreover, the comparator 124 receives a signal for comparison from the collector of the amplifier-transistor 112 through a pair of coupling transistors 128 and 130. When the signals in the comparator 124 do compare, an output is generated which is introduced into an inverter 132 for generating an output therefrom.

The output of the inverter 132 is then introduced into the control unit 14, which is more fully illustrated in FIG. 5 of the drawings. In this case, more specifically, the output from the receiver 12 is introduced into an exlusive NOR gate 140 which has an output to a microprocessor 142. The exclusive NOR gate 140 actually operates as an inverter. Moreover, it is preferably a programmable inverter. Furthermore, the microprocessor 142 receives a conductor carrying a reset input signal 144 from a reset signal generating circuit 145, as shown in FIG. 5. This reset signal generating circuit 145, which is sometimes referred to as a "watchdog" circuit, will automatically generate a reset signal each time that power is applied to the system, that is, each time that the system is "powered-up".

The reset signal generating circuit 145 may adopt any form of circuit which is capable of generating a reset signal. However, in the embodiment employed, a re-triggerable one-shot is connected to and operable in conjunction with a standard one-shot and capacitor. The capacitor may be committed to the standard one-shot through an NPN transistor and grounded. The collector of the NPN transistor would then be connected to the conductor 144. This arrangement has not been illustrated or described in any further detail herein inasmuch as any standard resetting circuit arrangement could be employed.

The microprocessor 142 also receives a plurality of input signals 146, 147, and 148, and where the input signal 148 represents a program signal or a signal from a program switch which may be located in the protected environment, as for example, the vehicle or dwelling structure or the like. The other inputs 146 and 147 into the microprocessor 142 are from sensors (not shown) and which sensors may adopt, for example, the form of a hood lock sensor, a vibration sensor, etc. Otherwise, other forms of input signals may be generated and introduced into the microprocessor 142 in the same manner as any of the signals 146.

The microprocessor 142 may be powered by means of a battery circuit 150, as shown in FIG. 5 and which comprises a conductor 152. The conductor 152 may be connected to a suitable 5-volt power source in the manner as shown. Also located in the conductor is an NPN transistor 154 which effectively functions as a diode to prevent current from moving back towards the 5-volt source and only enables current to be delivered to the microprocessor 142. The gate of the NPN transistor 154 is connected to the collector of another NPN transistor 156 in the manner as shown. The base of this transistor 156 is connected between a voltage dividing circuit 158 which controls the threshold voltage applied to the microprocessor 142. A battery 160 is connected to the conductor 152 through a resistor 162 and a diode 164 in the manner as illustrated. A grounding capacitor 166 is also connected to the conductor 152 in the manner as illustrated in FIG. 5.

The microprocessor 142 has a plurality of output signals 168 which are generally 4-volt signals and which are introduced into a buffer-amplifier 170. This buffer-amplifier 170 produces a plurality of outputs 172. Moreover, each of the outputs 172 are connected to a 12-volt power source through coupling resistors 174 in the manner as illustrated, such that the outputs are raised to 12 volts. Each of the amplified signals 172 are then introduced into output circuits 176 in the manner as illustrated in FIG. 5.

The output circuits of FIG. 5 each generally comprise a field-effect transistor 178 which is connected through diodes 180 to a 12-volt power source. The various outputs from the output circuits 176 may provide responsive functions in the protected environment. For example, a first output 176 may generate a siren. A second output may provide for a pulsed alarm. A third output may provide for an automatic door lock or an automatic unlocking of a door. Another output may provide for an ignition cut-off, that is, so that the ignition of a vehicle could not be started in the event of an intrusion or an unauthorized entry into the vehicle. Other forms of outputs could similarly be provided.

A special output from the microprocessor 142 in the form of a hood unlock signal is introduced into an inverter assembly 182 and then into an NPN transistor 184 which amplifies the signal. A coupling resistor 186 connects the base of the transistor 184 to the output of the inverter. Finally, the collector of the transistor 184 is connected to an output circuit 188 which is also comprised of a field effect transistor 190. This signal serves to automatically unlock the hood when generated. The generation of the hood unlock signal is authorizedly initiated by the control unit 14 of the system for a thirty-second time period after initially disarming the system.

Also connected to the microprocessor 142 is an oscillator control circuit 192 comprised of a crystal oscillator 194 and having a pair of capacitors 196 connected to the outputs thereof. This crystal oscillator 192 generates a control frequency which controls the speed of operation of the microprocessor 142 and generates the clocking signals therefore.

The microprocessor 142 also generates a plurality of control light outputs 198 which may control light emitting diodes 200 or other forms of light emitting devices. A pair of these signal light outputs may inform the user whether the system is turned on or off and a third of the signal light outputs 198 may inform the user if the microprocessor is running code in a correct sequence. It should be understood that other forms of output signal lights for generating other informational outputs may be employed in accordance with the present invention.

OPERATION OF THE SYSTEM

The operation of the security system has been described in connection with the detailed description thereof.

However, the following should provide a brief summary of the operation of the various embodiments of the system.

The encoder **16** may be operated by actuation of one of the switches **54** or **56**, as previously described. The encoder will thereupon generate a coded signal which is transmitted by the transmitter **10** as a radio frequency signal. The signal is then received by the receiver **12** and which will process the signal and generate an electrical signal output at the inverter **132**. The signal from the inverter **132** is introduced into and decoded in the control unit **14**, as aforesaid.

When the user desires to match a transmitter to the receiver, the receiver will first be placed in the program mode. This may be accomplished, as aforesaid, by enabling a switch in the receiver into a program position. The switch may be activated manually or electronically or through voice recognition. When the receiver is then in the program mode, any transmitter which is to have its signature control signal recorded therein is actuated to generate an encoded signal. This encoded signal will then be recorded as a signature control signal in the receiver-control unit. If only one transmitter is actuated, only a single signature control signal will be recorded in the receiver-control unit. If different transmitters are actuated when the receiver is in the program mode, each of those actuated transmitters will have its own signature control signal recorded. The receiver will exit the program mode automatically after a preset duration where the receiver is then in a condition to receive and decode subsequent encoded signals.

All subsequent signals will be compared against these signature control signals. If the subsequent signals are identical to the any of signature control signal, then they will be recognized as a valid encoded signal and will thereupon arm or disarm the security system. However, if they do not conform to the signature control signals which have been recorded, then the subsequently transmitted and decoded signals will not arm or disarm the security system.

As indicated previously, the transmitter may be capable of generating one or two individual encoded signals by actuation of the switches **54** and **56**. Thus, either of the encoded signals from a single transmitter may be used to operate the control unit. In like manner, the control unit could be operated in such manner that both encoded signals are required before the system can be armed or disarmed. In this way, the security of the system is further enhanced.

The user of the system can also easily delete one of the transmitters from the system by removing the signature control signal of that transmitter from the control unit. In this case, the signature control signal of the transmitter can be deleted from the system, depending upon the specific programming of the receiver-control unit. In one of the preferred embodiments, if the receiver is placed in the program mode and the signature control signal is generated on a plurality of successive occasions, such as four successive occasions in close sequence, that will cause an automatic deletion of the signature control signal and hence, that transmitter from the system.

In accordance with the above identified circuit arrangement it can be understood that it is not necessary for the user or the dealer, or the installer of the system to either understand or to have knowledge of the specific encoded signal which is generated in order to add or delete any transmitter from the remote control access system. Thus, the user does not have to actuate any predetermined number of switchs or other input means, such as scratch a circuit pattern on a printed circuit board in order to generate the encoded signal. Indeed, the user or dealer or installer does not have to possess and use any of the special techniques for encoding the transmitter and which usually requires the intervention of skilled personnel. Moreover, it is not even necessary for the user or the dealer or installer to open either the transmitter or the receiver in order to record the signature control signal.

When in the program mode and when a signal is transmitted from any one or more transmitters, that signal will be received by the receiver and decoded by the control unit. After decoding, the received signal will then be recorded in the memory of the control unit as a signature control signal. This will occur with each signal received from any transmitter when in the program mode. When the receiver is in the receive mode, no further recording can be accomplished until the receiver is switched back to the program mode. When in the receive mode, if any encoded signals are generated and received by the receiver, they will be decoded and compared against the recorded signature control signals which have been recorded in the memory unit. If there is no comparison with any signature control signal, the received signal will be recognized as an invalid signal and will not arm or disarm the system.

In accordance with the above-identified construction, it can be observed that additional transmitters can be added to or deleted from the system at will. Moreover, it is not necessary to have the intervention of skilled personnel, such as a dealer or installer, to add or delete the transmitter from the system inasmuch as this can be easily accomplished by the user of the system. The system of the invention is also highly effective in that it may be used with many transmitters and also many different types of transmitters and with transmitters operating on different coded bases. The use of the system with a plurality of differing types of transmitters is more fully illustrated in FIG. **2** of the drawings.

In this case, it can be observed that a first transmitter **10A** and associated encoder **16A** generate a first code **A1**. This transmitter **10A** and encoder **16A** will generate a second code **A2** if a pair of channels are provided on this transmitter-encoder combination. Thus, and for this purpose, the circuit arrangement of FIG. **3** would be employed utilizing both switches **54** and **56**. In like manner, a second transmitter-encoder combination comprised of a transmitter **10B** and an encoder **16B** are provided for purposes of generating a code **B1** and an encoded signal **B2**. Finally, a third transmitter-encoder combination comprised of a transmitter **10C** and an encoder **16C** are capable of generating a first encoded signal **C1** and a second encoded signal **C2**. As also indicated previously, any of these transmitters could be used with more or less than two channels for generating any desired number of codes.

In accordance with the arrangement as illustrated in FIG. **2**, it can be observed that each of these transmitters and encoders may be of different types and each will generate different encoding signals. Nevertheless, on the first occasion when each of these transmitters are used, they will be used in such manner so as to operate the control unit to record a signature control signal. Thus, each of the three transmitter-encoder combinations will have their signature control signal recorded in the control unit. On each subsequent occassion, when they are actuated, they will be capable of arming and dis-arming the security system, in the manner as previously described.

One of the unique aspects of this invention is the fact that any conventional transmitter can be used as long as it is operating on the same frequency as the receiver. Thus, if the user of the system loses one of the transmitters or desires to upgrade the system with another transmitter with more digital codes and higher security, it is not necessary to install an entirely new system. The user merely buys another transmitter and records the signature control signal in the microprocessor of the control unit 14.

Moreover, it is important to note that it is not necessary to have each transmitter, such as the transmitter-encoder combination illustrated in FIG. 2, to generate the same encoded signal. Thus, the user may merely provide additional authorized parties with transmitters for obtaining access to the security system without an elaborate time consuming and costly recording of a particular transmitter. It is necessary to only record once the signature control signal of that transmitter in the control unit, as aforesaid.

Another one of the unique aspects of the invention is that the encoded signal cannot be deciphered by electronic scanning techniques. As previously described, the microprocessor operated control unit generates a time delay between the processing of any received and decoded signal. Thus, if the first received and decoded signal is not a valid code, the microprocessor will generate a time delay before reading any other transmitted signal, and which time delay which is longer than the time required for a scanner to generate the necessary subsequent coded signals. Thus, if an electronic scanner is in operation each time that it transmits an invalid code it will disable the control unit. As the scanner steps through the various code possibilities, even when it transmits the correct code preceded and followed by an invalid code the microprocessor will not recognize the valid code since the previous invalid code will have caused an inhibiting of any subsequent reading of a code, whether or not a valid code, for a time period which is far too slow for any scanner stepping through successive codes. Thus, any valid code which is generated by the scanner would automatically be masked and not read by the receiver-control unit.

In accordance with the present invention, it is also possible to simultaneously use any number of coded combinations, as for example, a 14-bit encoded signal which could result in sixteen thousand encoded signal combinations. In like manner, it is possible to use a 20-bit signal which could result in up to one million encoded signal combinations, etc. In essence, the system of the present invention is virtually unlimited to the number of codes which can be used or the number of bits in any encoded signal.

The system of the invention is also capable of comparing two or more sequential encoded, transmitted and decoded signals to ensure that they are identical to one another. Thereafter, if the subsequently decoded signals are identical, they are then compared to the signature control signals. If the decoded signals match the signature control signal, then it is deemed to be a valid transmitted signal for purposes of arming or disarming the security system.

This arrangement for signal matching is more fully illustrated in FIG. 6 of the drawings. It can be observed that a signature control signal is shown in the upper portion of FIG. 6. The first of the bits, designated as 202 is a wider bit than another one of the bits 204 and thus, the bit 202 may represent, for example, a "1" signal, whereas the bit 204 may represent a "0" signal. Located beneath the signature signal is the transmitted signal which may have been decoded in the control unit. In this case, it can be observed that the transmitted signal is identical to the signature signal.

The transmitted signal has a length of n bits, in the manner as illustrated in FIG. 6. Located to the right of the transmitted signal is a second transmitted signal. In this case, it can be observed that the second transmitted signal is shown to be duplicate of the first transmitted signal. In this way, the two transmitted and decoded signals will compare in the comparator of the control unit. As a result, they will form a signal combination which may be compared against the signature control signal. In this case, it can be observed that the two transmitted signals are identical and are also identical to the signature control signal. As a result, the microprocessor operated control unit will recognize this as a valid decoded signal, enabling the user to have access to the security system for purposes of arming or disarming the same.

Contrarywise, it can also be observed, that if the second transmitted and decoded signal is not identical to the first transmitted signal, then there is no further comparison with respect to the signature control signal. There must be at least two or more sequential transmitted and decoded signals which are identical to one another before any comparison to the signature control signal can take place and hence, there must be the same comparison before any arming or disarming of the system can occur.

The microprocessor may also measure various other characteristics of the bits in order to determine whether or not a decoded signal is a valid signal. For example, the microprocessor could examine and compare bit length, the number of bits and the widths of the bits. Other characteristics, for example, amplitude or the like could also be used for determining whether a decoded signal is a proper or valid decoded signal.

Thus, there has been illustrated and described a unique and novel remote control radio frequency access system which includes many unique features, such as the fact that it can be operated by an encoded signal of which no person needs to have knowledge of the encoded signal for the purpose of coding the control unit and the fact that the transmitter does not need to be opened for coding. Moreover, the system can be operated by a plurality of transmitters, with each being of a different type and having different encoded signals and each may be added or deleted at will by the user. The system can also be operated in such manner that the code cannot be detected by electronic scanning. Thus, the present invention fulfills all of the objects and advantages which have been sought. It should be understood that many changes, modifications, variations and other uses and applications will become apparent to those skilled in the art after considering this specification and the accompanying drawings. Therefore, any and all such changes, modifications, variations and other uses and applications which do not depart from the spirit and scope of the invention are deemed to be covered by the invention which is limited only by the following claims.

Having thus described the invention, what I desire to claim and secure by letters patent is:

1. An electronically programmable remote control vehicle security system, comprising:

sensor apparatus mounted on said vehicle for detecting attempted intrusions to said vehicle;

vehicle antitheft apparatus;

a precoded remote control transmitter for generating and transmitting a non-user-programmable, digitally encoded radio frequency signal representative of a multiple-bit transmitter code, said transmitter including an actuator switch which when actuated by a user causes said digitally encoded radio frequency signal to be transmitted, said transmitter code being precoded so that a system user is not required to encode said transmitter or know said transmitter code;

a radio frequency receiver responsive to said radio frequency transmitter signal to provide receiver signals indicative of said transmitter code;

a system control unit disposed within said vehicle and having control over said vehicle antitheft apparatus, said control unit comprising:

a digital memory;

programming apparatus responsive to said receiver signals for recording in said memory only during a programming mode said transmitter code as a signature control signal for arming or disarming said vehicle antitheft apparatus;

operating apparatus operable during a system security operating mode and responsive to said receiver signals for comparing said receiver signals to said recorded signature control signal and arming said vehicle antitheft apparatus upon a first receipt and recognition of receiver signals corresponding to said signature control signal, and for disarming said antitheft apparatus upon a second receipt and recognition of receiver signals corresponding to said signature control signal.

2. The vehicle security system of claim 1 wherein said programming apparatus is operable in the program mode to record a plurality of different transmitter codes from a plurality of remote control transmitters as a plurality of different signature control signals, and wherein said operating apparatus is responsive to said receiver signals for comparing said receiver signals to each of said signature control signals to find a match, and arms said antitheft apparatus upon a first receipt and recognition of any one of said recorded signature control signals, and disarms said antitheft apparatus upon a second receipt and recognition of any one of said recorded signature control signals.

3. The vehicle security system of claim 1 wherein said system control unit includes a program switch disposed in said vehicle, and said system control unit is responsive to said switch for entering the program mode.

4. The vehicle security system of claim 1 wherein said remote control transmitter is encoded with said transmitter code by the manufacturer thereof.

5. The vehicle security system of claim 1 wherein operating apparatus is further responsive to intrusion attempt signals from said sensor apparatus for activating said vehicle antitheft apparatus upon tripping of said sensor apparatus only when said antitheft apparatus is armed.

6. The vehicle security system of claim 1 wherein said antitheft apparatus includes apparatus for disabling operation of said vehicle.

7. The vehicle security system of claim 6 wherein said apparatus for disabling operation of said vehicle includes circuitry for disabling an ignition system of said vehicle.

8. The vehicle security system of claim 1 wherein said antitheft apparatus includes an alarm device activated by said control unit for generating an alarm when an attempted intrusion is detected by said sensor apparatus while the antitheft apparatus is armed.

9. The vehicle security system of claim 1 wherein the operating apparatus is operable to perform a further function in addition to disarming said antitheft apparatus upon the second receipt and recognition of receiver signals corresponding to said signature control signal.

10. The vehicle security system of claim 9 wherein said further function includes unlocking a vehicle access location lock.

11. The vehicle security system of claim 1 further comprising apparatus for putting the system control unit in the programming mode without the use of the remote control transmitter code.

12. An electronically programmable remote control vehicle security system, comprising:

sensor apparatus mounted on said vehicle for detecting attempted intrusions to said vehicle;

vehicle antitheft apparatus;

a precoded remote control transmitter for generating and transmitting a non-user-programmable, digitally encoded radio frequency signal representative of a multiple-bit transmitter code, said transmitter including an actuator switch which when actuated by a user causes said digitally encoded radio frequency signal to be transmitted, said transmitter code being precoded so that a system user is not required to encode said transmitter or know said transmitter code;

a radio frequency receiver responsive to said radio frequency transmitter signal to provide receiver signals indicative of said transmitter code;

a system control unit disposed within said vehicle and having control over said vehicle antitheft apparatus, said control unit comprising:

a digital memory;

programming apparatus responsive to said receiver signals for recording in said memory only during a programming mode said transmitter code as a signature control signal for arming or disarming said vehicle antitheft apparatus;

operating apparatus operable during a system security operating mode and responsive to said receiver signals for comparing said receiver signals to said recorded signature control signal and arming or disarming said vehicle antitheft apparatus upon receipt and recognition of receiver signals corresponding to said signature control signal.

13. The vehicle security system of claim 12 wherein said remote control transmitter is encoded with said transmitter code by the manufacturer thereof.

14. A user programmable remote control vehicle security system, in which an encoded signal from a transmitter may be recorded as a signature control word and without a need for the user or an installer to have a knowledge of the encoded signal and which does not require access to the interior of the transmitter or receiver, said system comprising:

sensor apparatus mounted on said vehicle for detecting attempted intrusions to said vehicle;

vehicle antitheft apparatus;

a precoded remote control transmitter for generating and transmitting a non-user-programmable, digitally encoded radio frequency signal representative of a multiple-bit transmitter code, said transmitter including an actuator switch which when actuated by a user causes said digitally encoded radio frequency signal to be transmitted, said transmitter code being precoded so that a system user is not required to encode said transmitter or know said transmitter code;

a radio frequency receiver responsive to said radio frequency transmitter signal to provide receiver signals indicative of said transmitter code;

a system control unit disposed within said vehicle and having control over said vehicle antitheft apparatus, said control unit comprising:

a digital memory;

programming apparatus responsive to said receiver signals for recording in said memory only during a programming mode said transmitter code as a signature control signal for arming or disarming said vehicle antitheft apparatus, the programming apparatus in the programming mode requiring only the transmission of the encoded signal from the transmitter for recording as a signature control signal and thereby eliminating any need for access to the interior of the transmitter or receiver or control unit and thereby removes the need of the user or installer to have knowledge of the specific signature control signal;

operating apparatus operable during a system security operating mode and responsive to said receiver signals for comparing said receiver signals to said recorded signature control signal and arming or disarming said vehicle antitheft apparatus upon a receipt and recognition of receiver signals corresponding to said signature control signal.

15. The vehicle security system of claim **14** wherein said remote control transmitter is encoded with said transmitter code by the manufacturer thereof.

* * * * *

JS 44 (Rev. 11/04)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON THE REVERSE OF THE FORM.)

I. (a) PLAINTIFFS
DEI HEADQUARTERS, INC., a Florida Corporation

DEFENDANTS
AUTO PAGE, INC., a California Corporation, and ADVANCED SECURITY, INC., a Taiwan Corporation

FILED
2007 DEC 21 PM 4: 29
CLERK US DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
BY ____ DEPUTY

(b) County of Residence of First Listed Plaintiff San Diego
(EXCEPT IN U.S. PLAINTIFF CASES)

County of Residence of First Listed Los Angeles
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE LAND INVOLVED.

(c) Attorney's (Firm Name, Address, and Telephone Number)
Stephen S. Korniczky (135532), S. Christian Platt (199318),
Sam Talpalatsky (171292), Trevor Q. Coddington (243042)
Paul, Hastings, Janofsky & Walker LLP
3579 Valley Centre Drive
San Diego, CA 92130
(858) 720-2500

Attorneys (If Known)

'07 CV 2406 BTM RBB

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question (U.S. Government Not a Party)
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant) (For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT (Place an "X" in One Box Only)

CONTRACT
☐ 110 Insurance
☐ 120 Marine
☐ 130 Miller Act
☐ 140 Negotiable Instrument
☐ 150 Recovery of Overpayment & Enforcement of Judgment
☐ 151 Medicare Act
☐ 152 Recovery of Defaulted Student Loans (Excl. Veterans)
☐ 153 Recovery of Overpayment of Veteran's Benefits
☐ 160 Stockholders' Suits
☐ 190 Other Contract
☐ 195 Contract Product Liability
☐ 196 Franchise

REAL PROPERTY
☐ 210 Land Condemnation
☐ 220 Foreclosure
☐ 230 Rent Lease & Ejectment
☐ 240 Torts to Land
☐ 245 Tort Product Liability
☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
☐ 310 Airplane
☐ 315 Airplane Product Liability
☐ 320 Assault, Libel & Slander
☐ 330 Federal Employers' Liability
☐ 340 Marine
☐ 345 Marine Product Liability
☐ 350 Motor Vehicle
☐ 355 Motor Vehicle Product Liability
☐ 360 Other Personal Injury

PERSONAL INJURY
☐ 362 Personal Injury—Med. Malpractice
☐ 365 Personal Injury — Product Liability
☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
☐ 370 Other Fraud
☐ 371 Truth in Lending
☐ 380 Other Personal Property Damage
☐ 385 Property Damage Product Liability

CIVIL RIGHTS
☐ 441 Voting
☐ 442 Employment
☐ 443 Housing/ Accommodations
☐ 444 Welfare
☐ 445 Amer. w/Disabilities - Employment
☐ 446 Amer. w/Disabilities - Other
☐ 440 Other Civil Rights

PRISONER PETITIONS
☐ 510 Motions to Vacate Sentence
Habeas Corpus:
☐ 530 General
☐ 535 Death Penalty
☐ 540 Mandamus & Other
☐ 550 Civil Rights
☐ 555 Prison Condition

FORFEITURE/PENALTY
☐ 610 Agriculture
☐ 620 Other Food & Drug
☐ 625 Drug Related Seizure of Property 21 USC 881
☐ 630 Liquor Laws
☐ 640 R.R. & Truck
☐ 650 Airline Regs.
☐ 660 Occupational Safety/Health
☐ 690 Other

LABOR
☐ 710 Fair Labor Standards Act
☐ 720 Labor/Mgmt. Relations
☐ 730 Labor/Mgmt.Reporting & Disclosure Act
☐ 740 Railway Labor Act
☐ 790 Other Labor Litigation
☐ 791 Empl. Ret. Inc. Security Act

BANKRUPTCY
☐ 422 Appeal 28 USC 158
☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
☐ 820 Copyrights
☒ 830 Patent
☐ 840 Trademark

SOCIAL SECURITY
☐ 861 HIA (1395ff)
☐ 862 Black Lung (923)
☐ 863 DIWC/DIWW (405(g))
☐ 864 SSID Title XVI
☐ 865 RSI (405(g))

FEDERAL TAX SUITS
☐ 870 Taxes (U.S. Plaintiff or Defendant)
☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
☐ 400 State Reapportionment
☐ 410 Antitrust
☐ 430 Banks and Banking
☐ 450 Commerce
☐ 460 Deportation
☐ 470 Racketeer Influenced and Corrupt Organizations
☐ 480 Consumer Credit
☐ 490 Cable/Sat TV
☐ 810 Selective Service
☐ 850 Securities/Commodities/ Exchange
☐ 875 Customer Challenge 12 USC 3410
☐ 890 Other Statutory Actions
☐ 891 Agricultural Acts
☐ 892 Economic Stabilization Act
☐ 893 Environmental Matters
☐ 894 Energy Allocation Act
☐ 895 Freedom of Information Act
☐ 900 Appeal of Fee Determination Under Equal Access to Justice
☐ 950 Constitutionality of State Statutes

V. ORIGIN (Place an "X" in One Box Only)

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from another district (specify) ☐ 6 Multidistrict Litigation ☐ 7 Appeal to District Judge from Magistrate Judgment

VI. CAUSE OF ACTION
Cite the U.S. Civil Statute under which you are filing **(Do not cite jurisdictional statutes unless diversity):**
35 U.S.C. § 271 et seq.
Brief description of cause:
Complaint for Patent Infringement

VII. REQUESTED IN COMPLAINT:
☐ CHECK IF THIS IS A CLASS ACTION UNDER F.R.C.P. 23
DEMAND $
CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY (See instructions): JUDGE ______ DOCKET NUMBER ______

DATE
December 21, 2007
SIGNATURE OF ATTORNEY OF RECORD
[signature]

FOR OFFICE USE ONLY

RECEIPT # 145842 AMOUNT $350 12/21/07-BSL APPLYING IFP ______ JUDGE ______ MAG. JUDGE ______

UNITED STATES
DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
SAN DIEGO DIVISION

# 145842 - BH

December 21, 2007
16:33:51

Civ Fil Non-Pris
USAO #.: 07CV2406 CIVIL FILING
Judge..: BARRY T MOSKOWITZ
Amount.: $350.00 CK
Check#.: BC# 0038010

Total-> $350.00

FROM: CIVIL FILING
DEI HEADQUARTERS V. AUTO PAGE